VDAB
TRAINING & OPLEIDING

Samen sterk voor werk

# Windows Server Administration

## Active directory

# Inhoud

**1 ACTIVE DIRECTORY DOMAIN SERVICES ..... 4**

**1.1 AD DS, EEN NETWERKDIRECTORY. ..... 4**
**1.2 DE STRUCTUUR VAN AD DS ..... 5**
**1.3 LOGISCHE BOUWSTENEN ..... 7**
1.3.1 HET GLOBALE PLAATJE ..... 7
1.3.2 FORESTS ..... 8
1.3.3 DOMEINEN ..... 9
1.3.4 TREES ..... 10
1.3.5 VERTROUWENSRELATIES ..... 10
1.3.6 ORGANIZATIONAL UNITS (OU) ..... 11
**1.4 REPLICATIE VAN AD DS ..... 11**
1.4.1 DE SCHEMAPARTITIE ..... 11
1.4.2 DE CONFIGURATIEPARTITIE ..... 11
1.4.3 DE DOMEINPARTITIE ..... 11
1.4.4 DE APPLICATIEPARTITIE ..... 12
1.4.5 DE GLOBAL CATALOG SERVER ..... 12
1.4.6 FSMO ROLLEN ..... 12
**1.5 SITES ..... 15**
**1.6 FUNCTIONAL LEVELS ..... 16**
**1.7 AUTHENTICATIE ..... 17**
1.7.1 AANMELDEN ..... 17
1.7.2 KERBEROS ..... 17
**1.8 ROLES AND FEATURES ..... 19**

**2 INSTALLATIE VAN WINDOWS SERVER ..... 20**

**2.1 HARWAREVEREISTEN ..... 20**
**2.2 INSTALLATIE VAN HET SERVERBESTURINGSSYSTEEM ..... 21**

**3 INITIËLE CONFIGURATIE NA INSTALLATIE ..... 25**

**3.1 DE COMPUTERNAAM ..... 25**
**3.2 HET DOMEIN ..... 26**
**3.3 WINDOWS FIREWALL ..... 26**
**3.4 REMOTE MANAGEMENT ..... 26**
**3.5 REMOTE DESKTOP ..... 27**
**3.6 NIC TEAMING ..... 28**
**3.7 ETHERNET ..... 28**
**3.8 UPDATES ..... 29**
**3.9 WINDOWS DEFENDER ..... 29**
**3.10 FEEDBACK & DIAGNOSTICS ..... 30**
**3.11 TIME ZONE ..... 30**
**3.12 PRODUCT ID ..... 30**

**4 EEN DOMEINCONTROLLER INSTALLEREN ..... 31**

**4.1 DE ROL VAN DNS ..... 31**
4.1.1 HET BELANG VAN DNS ..... 31

4.1.2 ENKELE TYPES VAN DNS-RECORD ..... 32
4.1.3 DNS INSTALLEREN ..... 33
4.1.4 DE DNS SERVER KENBAAR MAKEN ..... 33
**4.2 INSTALLATIE VAN ACTIVE DIRECTORY DOMAIN SERVICES IN DE PRAKTIJK ..... 34**
4.2.1 INSTALLATIE VAN DE AD DS ROLE ..... 34
4.2.2 DCPROMO ..... 36
4.2.3 CONTROLE VAN DE INSTALLATIE ..... 37
**4.3 CLIENTS LID MAKEN VAN HET DOMEIN ..... 39**
4.3.1 EEN CLIENT MET STATISCHE IP-INSTELLINGEN ..... 40
4.3.2 EEN CLIENT MET DYNAMISCHE IP-INSTELLINGEN ..... 41

**5 APPENDIX: NAAMRESOLUTIE - DNS ..... 47**

**5.1 NAAMRUIMTES ..... 47**
5.1.1 VLAKKE NAAMRUIMTES ..... 47
5.1.2 HIËRARCHISCH GESTRUCTUREERDE NAAMRUIMTES ..... 47
**5.2 NAAMREGISTRATIE ..... 48**
**5.3 NAAMRESOLUTIE MET EEN HOSTSBESTAND ..... 48**
**5.4 NAAMRESOLUTIE MET DNS ..... 49**
5.4.1 DE STRUCTUUR ACHTER DNS ..... 49
5.4.2 ZONES EN DOMEINEN ..... 51
5.4.3 RECORDS ..... 52
5.4.4 HOE GEBEURT EEN DNS NAAMOMZETTING? ..... 53
5.4.5 IP ADRESSEN OMZETTEN IN NAMEN ..... 56

**6 COLOFON ..... 57**

# 1 ACTIVE DIRECTORY DOMAIN SERVICES[1]

## 1.1 AD DS, een netwerkdirectory.

Netwerken ontstonden oorspronkelijk als een middel om op een eenvoudige manier randapparaten en schijfruimte te delen.

Vandaag controleren netwerken echter de meest uiteenlopende zaken van de uitbetaling van personeelsleden tot het verzenden van e-mails.

In de zoektocht om het beheer van een netwerk zo eenvoudig mogelijk te maken zijn de netwerken geëvolueerd van peer to peer netwerken tot netwerken waarvan het beheer via een directory gebeurt.

De implementatie van Microsoft van de X.500 standaard, een standaard ontwikkeld door IEEE[2] om via een directory een efficiënt beheer van een netwerk mogelijk te maken, is Active Directory Domain Services (AD DS).

Een directory is een database die geoptimaliseerd is om geraadpleegd te worden, m.a.w. de objecten die opgeslagen worden in de database zijn bij voorkeur niet voortdurend onderhevig aan verandering. Dit staat in tegenstelling tot b.v. een relationele database die geoptimaliseerd is om met regelmatig veranderende gegevens te werken.

In de database wordt informatie opgeslagen i.v.m. alle objecten in het netwerk o.a. gebruikers, computers, printers, …

De opgeslagen informatie hoeft zich niet te beperken tot informatie die met het netwerk te maken heeft, maar kan van allerlei aard zijn. Zo vind je naast de logon gegevens van een gebruiker in de AD DS ook zijn persoonlijk adres, telefoonnummer, GSM nummer, webpagina, ….

Een directory service maakt het mogelijk de gegevens in de database te raadplegen.

Enkele andere gekende uitvoeringen van netwerk directory services zijn

- eDirectory, ook wel bekend als NDS en gebruikt in Novell-netwerken
- Fedora Directory Server, ondersteund door Red Hat
- OpenLDAP (opensourcesoftware voor diverse besturingssystemen)
- Network Information Service (NIS) uit de omgeving van Unix-netwerken (niet op LDAP gebaseerd)
- Sun Java Directory
- Metadirectory door Critical Path, …

[1] Vanaf Windows 2008 Server krijgt wat in eerdere versies kortweg Active Directory genoemd werd, de naam Active Directory Domain Services of kortweg AD DS.

[2] IEEE of Institute of Electrical and Electronic Engineers, een Amerikaanse organisatie die zich onder andere met de formulering van LAN-normen bezighoudt.

AD DS maakt in tegenstelling tot deze andere directory services integraal deel uit van het besturingssysteem.

De database heeft een hiërarchische structuur gebaseerd op de naamgeving van de verschillende domeinen.

Ter vergelijking: de hiërarchische structuur van een (papieren) telefoonboek. Vertrek van een telefoonboek voor het hele land. Om te vermijden dat het opzoeken van een telefoonnummer te lang gaat duren, worden de namen van alle inwoners niet onmiddellijk alfabetisch gerangschikt, maar worden ze eerst gegroepeerd per provincie en dan binnen de provincie per gemeente. Om het telefoonnummer van iemand op te zoeken, ga je dan eerst op zoek naar de juiste provincie, vervolgens naar de gewenste gemeente en dan pas naar de naam.

Dit heeft gevolgen voor de naamgeving van de objecten: je gaat in het telefoonboek eigenlijk niet op zoek naar b.v. de naam Peeters zonder meer, maar naar de naam *Peeters.Deurne.Antwerpen.be*. Zo zal een computer in AD DS ook niet zonder meer Server0 heten, maar b.v. *Server0.opleidingen.intra* als die computer thuishoort in het domein opleidingen.intra. Op analoge wijze zal een gebruiker niet zonder meer de username Jean krijgen, maar *Jean.opleidingen.intra*. Verderop meer over domeinen.

De naam van een object in een domein gaat zo erg lijken op een URL, de naam van een site op het Internet. Op het Internet zorgt DNS (Domain Name System) ervoor dat je aan de hand van de URL het toestel vindt waarop een site aangeboden wordt. Ook bij AD DS gaat DNS een cruciale rol spelen om objecten op basis van hun naam terug te vinden in het netwerk.

## 1.2 De structuur van AD DS[3]

In AD DS zijn alle objecten zoals gebruikers, computers, printers, … terug te vinden die deel uitmaken van het netwerk.

Elk object wordt aangemaakt op basis van een object klasse. Een object klasse is dus eigenlijk een model van een object.

Een object klasse is op zijn beurt opgebouwd uit attributen. In de X.500 standaard is voor elk attribuut een uniek identificatienummer vastgelegd samen met een aantal eigenschappen, waaronder een naam en welke waarden het attribuut kan aannemen.

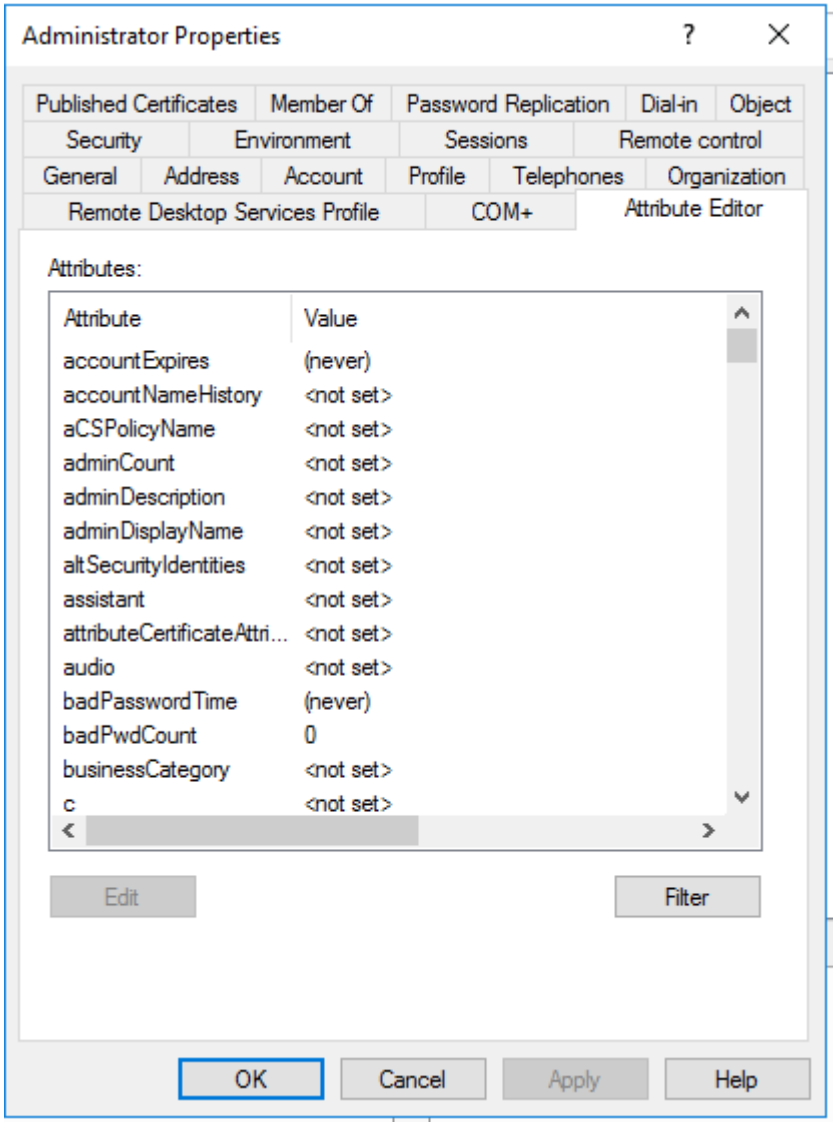
Het schema definieert de attributen die kunnen gebruikt worden om in AD DS objecten van een bepaalde klasse te creëren. Het is dus eigenlijk een lijst van alle klassen en attributen die in AD DS kunnen gebruikt worden.

[3] De micro structuur of de interne structuur

Enkele voorbeelden

| | |
|---|---|
| Objectklasse | User |
| Object van de klasse user | een welbepaalde gebruiker, b.v. Jean, User01, … |
| Enkele attributen van een object van de klasse user | name, givenName, accountExpires, badPwdCount, |

De verschillende attributen die bij een gebruiker horen, vind je terug via het tabblad Attribute Editor bij de eigenschappen van een gebruiker.



## 1.3 Logische bouwstenen[4]

AD DS kan al snel een grote database worden, die bovendien op een efficiënte manier moet kunnen gerepliceerd, geraadpleegd, beveiligd en beheerd worden. Een doordacht logisch ontwerp is dan ook erg belangrijk.

Beschikbare logische bouwstenen zijn daarbij domeinen, trees, forests en organizational units (OU).

### 1.3.1 Het globale plaatje

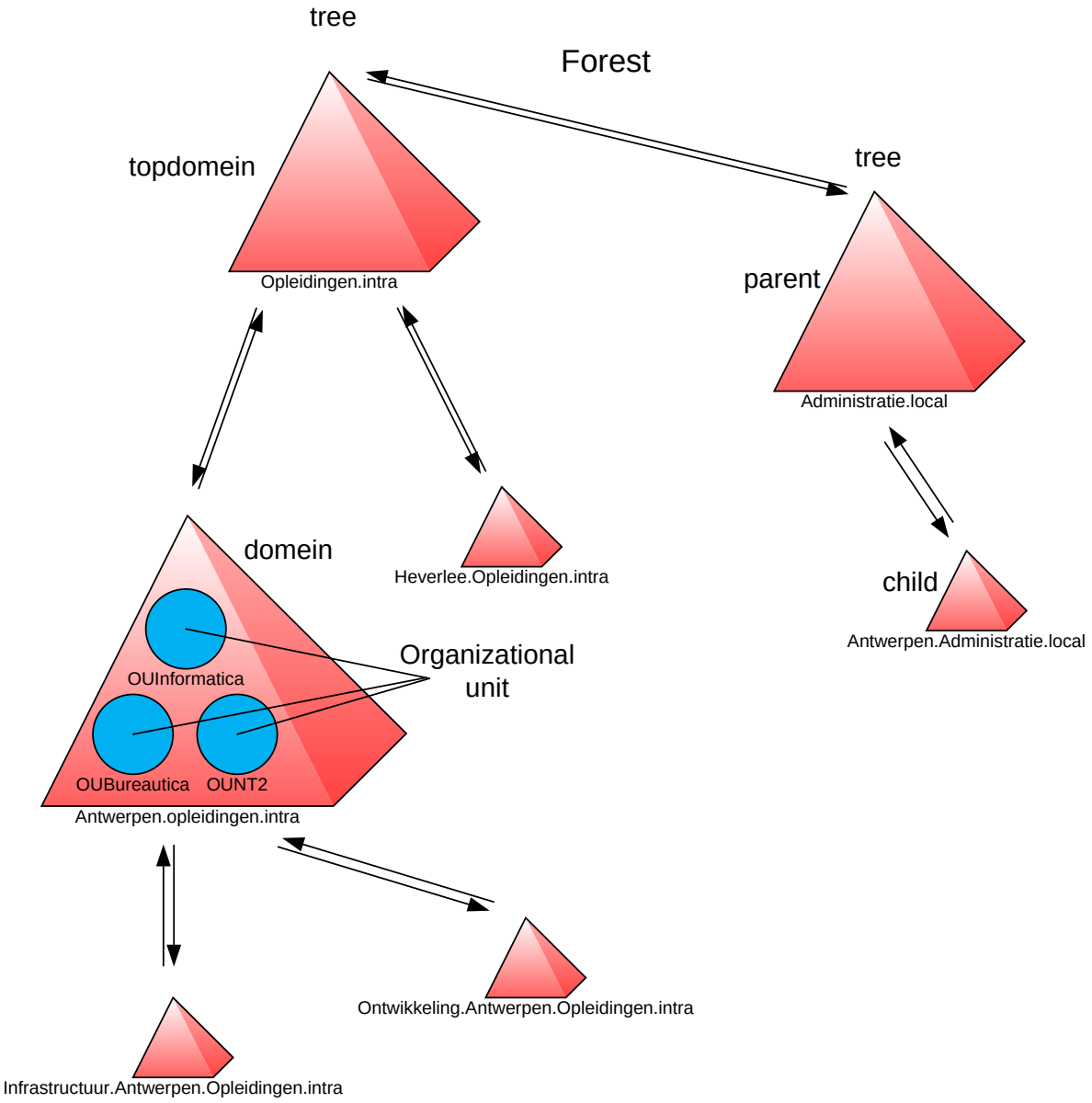
Een AD DS komt overeen met een forest. Een forest kan samengesteld zijn uit één of meerdere trees. In een tree vind je één of meerdere domeinen. Een domein kan dan nog verder opgedeeld worden in organizational units.

Hieronder vind je de schematische voorstelling van een forest met als topdomein Opleidingen.intra.

Binnen het forest bestaan twee trees: één met naamruimte Opleidingen.intra en één met naamruimte Administratie.local.

In de eerste tree vind je onder het topdomein nog twee child domeinen: Antwerpen.Opleidingen.intra en Heverlee.Opleidingen.intra. In de tweede tree vind je onder het domein Administratie.local nog een child domein Antwerpen.Administratie.local.

[4] De macro structuur




Binnen een domein kan je verder structureren met Organizational units.

Overwegingen i.v.m. beheer, replicatie en beveiliging zullen een belangrijke rol spelen bij het maken van keuzes i.v.m. het aantal forests, domeinen en organizational units.

### 1.3.2 Forests

Bij elk forest hoort één AD DS en omgekeerd hoort een AD DS bij één forest. In de meeste gevallen zal een netwerk van een bedrijf overeenkomen met één forest.

#### 1.3.2.1 Forests en beheer

De eerste beheerder van het eerste domein dat opgezet wordt in een forest, is automatisch ook lid van de enterprise administrators en krijgt daardoor beheerrechten op alle domeinen in het forest. Andere beheerders krijgen standaard alleen beheerrechten op hun eigen domein.

#### 1.3.2.2 De voor- en nadelen van meerdere forests

Zonder duidelijk aanwijsbare redenen is een structuur met één forest aan te raden. Dat zal het beheer, het onderhoud en het opsporen van problemen zeker vereenvoudigen. Toch zijn er ook argumenten om voor meerdere forests binnen eenzelfde netwerk te kiezen. Hieronder enkele voorbeelden.

- Een apart forest binnen een netwerk waar beheerders nieuwe configuraties voor het netwerk kunnen uitproberen alvorens ze geïmplementeerd worden
- Een apart forest waar ontwikkelaars hun software kunnen uitproberen
- Services of erg gevoelige data die geïsoleerd moeten blijven of die niet door alle beheerders mogen beheerd worden

### 1.3.3 Domeinen

In elk forest vind je minstens één domein.

Elk domein beschikt over een eigen database met gebruikers, computers, enz. Een server waarop deze database bestaat en beheerd wordt, is een domeincontroller.

Een domein is dus een verzameling resources en gebruikers die centraal kunnen beheerd worden aan de hand van één enkele database.

Enerzijds beschikt elk domein over ten minste één domeincontroller. Anderzijds kan een domeincontroller slechts bij één domein horen.

Twee of meer domeincontrollers op eenzelfde domein zijn aan te raden omwille van fouttolerantie en om de werkdruk te spreiden op drukke momenten. Zij beschikken dan allemaal over een identiek exemplaar van de database. Deze exemplaren worden gelijk gehouden via multimasterreplicatie, d.w.z. dat wijzigingen aan de database kunnen doorgevoerd worden op eender welke domeincontroller. Achteraf worden zij gerepliceerd naar alle andere domeincontrollers in het domein.

Ook voor domeinen geldt het principe, hoe minder domeinen hoe eenvoudiger het beheer.

#### 1.3.3.1 Domeinen en beheer

Zoals hiervoor al eens vermeld, heeft een enterprise administrator beheerrechten op alle domeinen in een forest. Daarnaast hoort bij elk domein ook een domein administrator die het recht heeft alle beheertaken op het domein uit te voeren.

#### 1.3.3.2 De voor- en nadelen van meerdere domeinen

Hoe meer domeinen opgezet worden in een netwerk, hoe ingewikkelder het beheer wordt. Dus ook hier gaat de voorkeur uit naar een structuur met slechts één domein.

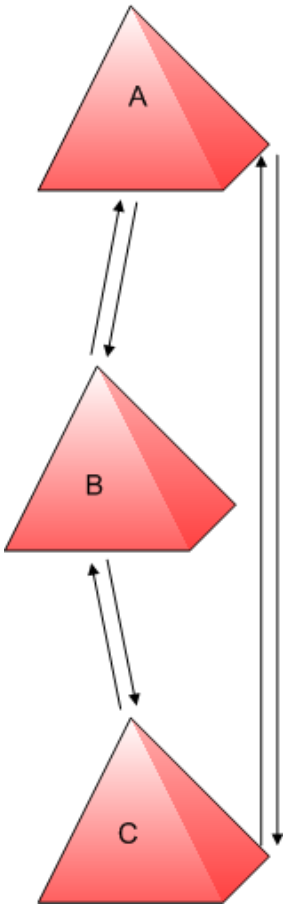
Toch kan het opzetten van meerdere domeinen nuttig zijn:

- Delen van het netwerk die door verschillende onafhankelijke personen moeten beheerd worden.

- Beperking van het replicatieverkeer. Hoe groter een domein wordt hoe meer replicatieverkeer er zal zijn binnen het domein. Binnen een domein is er meer replicatieverkeer nodig dan over domeinen heen.
- Delen van het netwerk waartussen het netwerkverkeer trager verloopt. Aangezien binnen een domein meer replicatieverkeer gebeurt dan over domeinen heen, kan zo het verkeer over de trage verbinding beperkt blijven.
- Beperking van de grootte van de AD Database

### 1.3.4 Trees

Een tree is een hiërarchisch gestructureerde verzameling domeinen in een eenzelfde naamruimte[5]. Domein A wordt in deze structuur de parent van domein B genoemd. Omgekeerd is domein B een child van domein A.




Binnen de meeste organisaties zal één naamruimte volstaan. Een tweede tree biedt de mogelijkheid om een tweede naamruimte te creëren binnen eenzelfde forest. Elke tree in een forest gebruikt een gemeenschappelijk schema en valt onder de bevoegdheid van de enterprise administrators.

### 1.3.5 Vertrouwensrelaties

Vertrouwensrelaties zorgen ervoor dat een gebruiker van een domein ook toegang heeft tot bestanden (en meer algemeen resources) in een gedeelde map in een ander domein binnen hetzelfde forest.

Windows Server maakt automatisch symmetrische en transitieve vertrouwensrelaties aan tussen parents en children.

Symmetrisch betekent in deze context dat een gebruiker van domein A, mits de nodige toegangsrechten, gedeelde mappen op domein B kan benaderen en omgekeerd dat een gebruiker van domein B, ook weer mits de nodige toegangsrechten, gedeelde mappen op domein A kan benaderen.

Transitief betekent dan weer dat als domein B domein A vertrouwt en domein C domein B vertrouwt, domein C automatisch ook domein A vertrouwt.
Het resultaat is dat een gebruiker van een domein in een tree aan gedeelde mappen kan op eender welk ander domein binnen die tree (mits de juiste toegangsrechten).

Het besturingssysteem zorgt ook voor wederzijdse vertrouwensrelaties tussen de topdomeinen van verschillende trees. Op die manier kan een gebruiker van eender welk domein terecht op alle andere domeinen in het forest.

[5] Een naamruimte is een logisch begrensd gebied dat namen bevat op basis van gestandaardiseerde afspraken om objecten of gegevens te representeren.

Tussen de topdomeinen van verschillende forests wordt standaard geen vertrouwensrelatie gelegd. Een enterprise administrator kan die wel zelf aanmaken.

### 1.3.6 Organizational units (OU)

In functie van het beheer kan een domein verder onderverdeeld worden in organizational units. De OU is een sleutelcomponent van het X.500 protocol.

Drie factoren spelen een rol bij het ontwerpen van OU's

- Objecten groeperen waarvan het beheer kan gedelegeerd worden
- Structuur brengen in de verzameling objecten van het domein
- Policies die moeten gelden voor bepaalde gebruikers en computers

OU's komen in één van de volgende hoofdstukken meer uitgebreid aan bod.

## 1.4 Replicatie van AD DS

Om de replicatie van AD DS in goede banen te leiden, wordt de database opgedeeld in vier partities:

- een schemapartitie
- een configuratiepartitie
- een domeinpartitie
- een applicatiepartitie

Bij elke partitie hoort een eigen replicatietopologie.

### 1.4.1 De schemapartitie

Deze partitie bevat het schema m.a.w. hier wordt de definitie opgeslagen van alle objecten en attributen die kunnen voorkomen in de AD DS samen met de spelregels om die objecten en attributen aan te maken en te manipuleren. De schemapartitie is op alle domeincontrollers in een forest identiek.

### 1.4.2 De configuratiepartitie

In de configuratiepartitie wordt de logische structuur van het netwerk opgeslagen. Welke domeinen zijn er en hoe passen die in de structuur? (zie ook 1.3 Logische bouwstenen).

Toepassingen die kunnen samenwerken met AD DS zoals Exchange en SQL server kunnen hier configuratie-informatie kwijt.

Ook de configuratiepartitie is identiek op alle domeincontrollers in een forest.

### 1.4.3 De domeinpartitie

De domeinpartitie houdt de gegevens van gebruikers, computers enz. bij die deel uitmaken van het domein. Zij wordt gerepliceerd naar alle domeincontrollers binnen een domein. Binnen een forest bestaan dus evenveel verschillende domeinpartities als er domeinen zijn.

### 1.4.4 De applicatiepartitie

Een applicatiepartitie wordt, in tegenstelling tot een domeinpartitie, alleen naar welbepaalde domeincontrollers gerepliceerd. Applicaties en services maken meestal zelf een applicatiepartitie aan om er hun objecten in op te slaan. Deze objecten mogen van eender welk type zijn, maar geen security principals. Een voorbeeld van een toepassing die met een applicatiepartitie werkt is DNS.

### 1.4.5 De Global Catalog Server

Elk forest beschikt ook over minstens één global catalog server. Fysiek gesproken worden de objecten per domein in de domeinpartitie opgeslagen. De Global Catalog (GC) zorgt ervoor dat de inhoud van al deze aparte databases toch als één geheel kan geraadpleegd worden. Voor de buitenwereld lijkt het dus alsof er maar één database voor heel het netwerk bestaat.

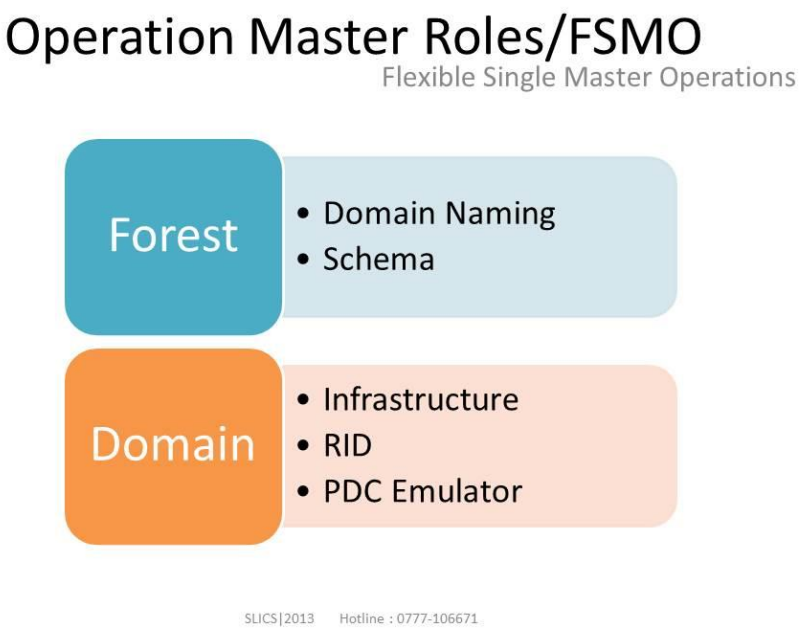
Om te vermijden dat de GC te groot en daardoor onhandelbaar wordt, bevat de GC echter niet van alle attributen van elk object op het netwerk een kopie, maar alleen van de meest geraadpleegde attributen.

Standaard wordt de eerste domein controller die in een forest opgezet wordt ook meteen Global Catalog Server.

### 1.4.6 FSMO rollen

Niet alle wijzigingen in Active Directory lenen zich tot multi-master replicatie. De verantwoordelijkheid voor het correct doorvoeren van dergelijke wijzigingen wordt dan ook toegewezen aan één welbepaalde domeincontroller. Men zegt dat die domeincontroller een FSMO (Flexible Single Master Operations) of Operations master rol opneemt.

Sommige FSMO rollen worden opgenomen voor het volledige forest, andere per domein.




Bron: http://microsoftserverhelp.blogspot.com

#### 1.4.6.1 Schema master

Per forest is er slechts één schema gedefinieerd. Wijzigingen aan het schema worden altijd via de schema master doorgevoerd. Er kan dus slechts één schema master zijn in een forest.

Via PowerShell kan je de schema master opvragen met de opdracht

```
Get-ADForest | select SchemaMaster
```

#### 1.4.6.2 Domain naming master

De domain naming master is o.a. verantwoordelijk voor het uniek zijn van de NETBIOS domeinnamen in het forest. Elke wijziging aan domeinnamen kan alleen doorgevoerd worden via de DC met deze rol. Ook het toevoegen of verwijderen van applicatie partities kan uitsluitend via de domeincontroller met deze rol. Deze rol kan slechts door één domeincontroller in het forest opgenomen worden.

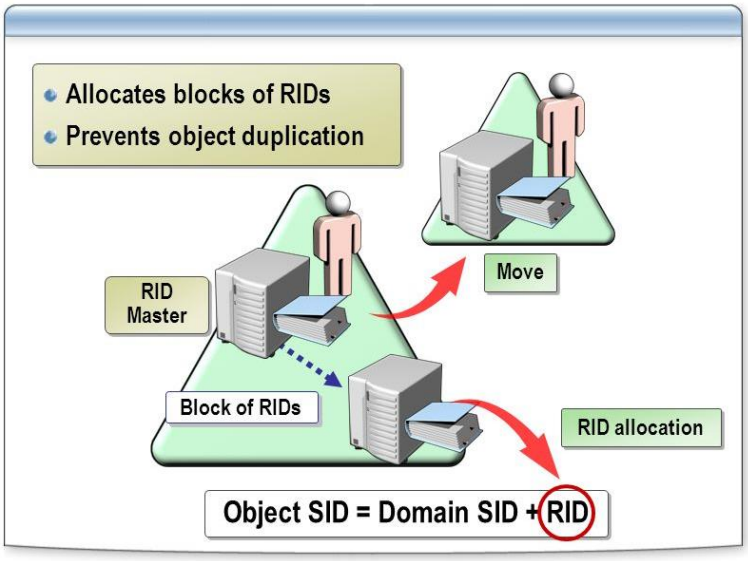
Met welke PowerShell opdracht denk je dat je de DomainNamingMaster opvraagt?

#### 1.4.6.3 Infrastructuur master

Per domein neemt één domeincontroller de rol van infrastructuur master op zich. Die volgt wijzigingen op in de eigenschappen van objecten van andere domeinen binnen het forest. Hij vergelijkt daartoe de SID en DN waarden van die objecten met de waarden in de global catalog en past indien nodig de waarden aan in zijn eigen database. De nieuwe waarden worden dan verder gerepliceerd naar de andere domeincontrollers binnen het domein.

### 1.4.6.4 RID master

De RID master beheert een verzameling relatieve identificatienummers die kunnen gebruikt worden bij het genereren van een SID voor een nieuw object op het domein. In geval er meerdere domeincontrollers op eenzelfde domein bestaan zal de RID master een reeks van 500 RID waarden ter beschikking stellen aan elke domeincontroller. Een domeincontroller die 50% van zijn RID waarden heeft gebruikt zal een volgende reeks waarden aanvragen bij de RID master.




```
Get-ADDomain | select RIDMaster
```

toont het toestel dat binnen een domein de rol van RID master op zich heeft genomen.

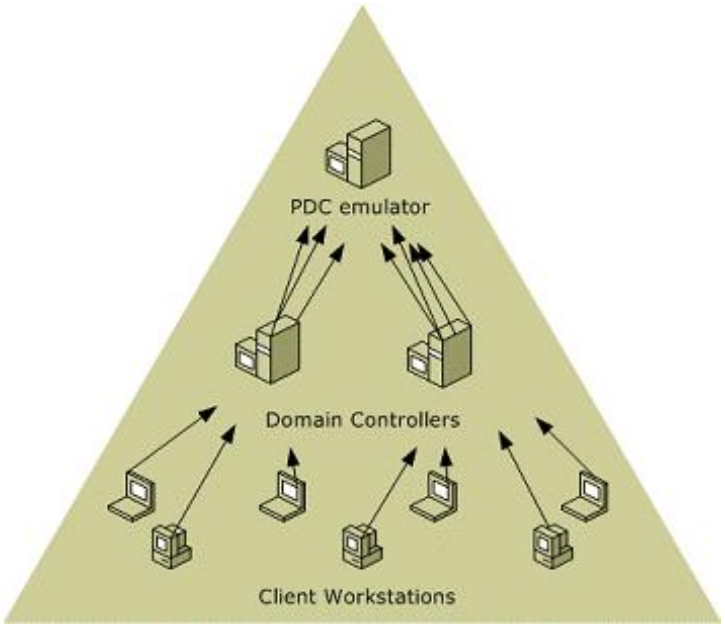
### 1.4.6.5 PDC emulator

In elk domein vind je een Primary domain controller emulator.

De PDC is verantwoordelijk voor de tijdsynchronisatie. Om authenticatie mogelijk te maken is het belangrijk dat alle domeincontrollers, computers en servers in een Active Directory domain dezelfde systeemtijd hebben. Een verschil van meer dan vijf minuten zal aanmelden onmogelijk maken.

De synchronisatie verloopt als volgt:

Computers en servers synchroniseren met de DC die hen geauthenticeerd heeft. Alle DC's synchroniseren op hun beurt met de PDC emulator. De PDC emulator synchroniseert met de PDC van het topdomein die op zijn beurt voor de juiste tijd te rade gaat bij een externe tijdserver.




Bron: http://techgenix.com/fsmo-roles-in-active-directory/

Daarnaast is de PDC ook verantwoordelijk voor het opvolgen van wachtwoord wijzigingen en het uitschakelen van een account waarvoor te veel foutieve wachtwoorden ingevoerd werden. Wijzigingen aan een group policy object worden doorgevoerd in de kopie van het group policy object die opgeslagen is in de sysvol map op de PDC.

Opvragen welk toestel de PDC is kan met de opdracht

```
Get-ADDomain | select PDCEmulator
```

## 1.5 Sites

Alle replicatie waarover tot nog toe gesproken werd, gebeurt standaard volledig automatisch en op initiatief van het besturingssysteem. Om het replicatieverkeer zelf te kunnen beheren zal een administrator met sites moeten werken.

In eenzelfde site horen alleen servers thuis die met elkaar verbonden zijn via een snelle en goede verbinding.

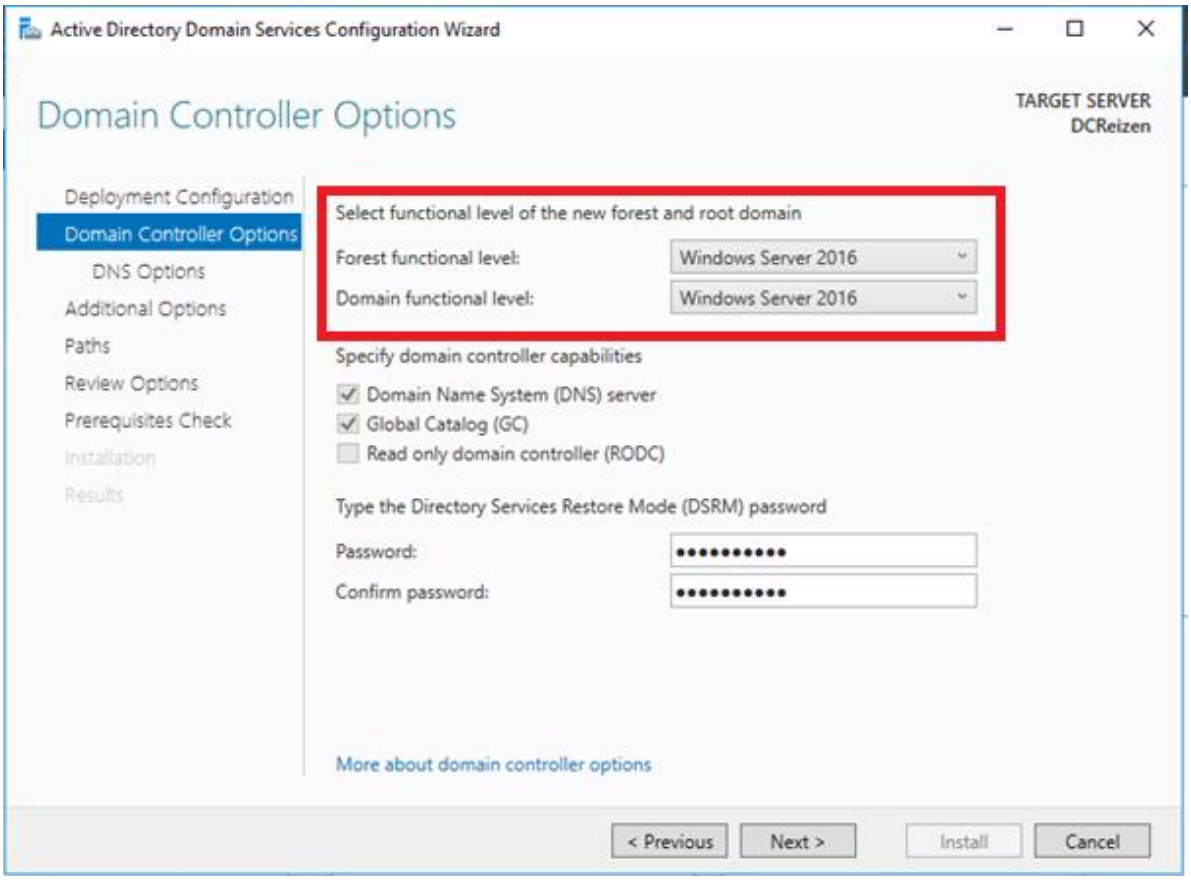
Replicatie tussen domeincontrollers die deel uitmaken van eenzelfde site gebeurt snel en frequent en op initiatief van het besturingssysteem. Replicatie tussen domeincontrollers in verschillende sites kan volgens een door de administrator gemaakte planning gebeuren.

Een tweede voordeel van sites is dat ook het verkeer tussen clients en servers tot een site kan beperkt worden. Als er een domeincontroller in dezelfde site ter beschikking is als de clientcomputer waarop een gebruiker zich probeert aan te melden, dan zal de authenticatie afgehandeld worden door de domeincontroller in die site.

Sites dragen verder ook bij tot een efficiënt gebruik van Distributed File System (DFS). (Zie hoofdstuk ‘Windows Server als fileserver’).

## 1.6 Functional levels

Elke nieuwe versie van Windows Server brengt nieuwe functionaliteiten mee. Domeincontrollers waarop nog een oudere versie van het besturingssysteem draait kunnen deze nieuwe mogelijkheden niet aan. Om compatibiliteit met de oudere versies te garanderen werkt Microsoft met functional levels zowel voor het domein als voor het forest.




Hoe lager het functional level hoe minder functionaliteiten van de laatste versie van het besturingssysteem ter beschikking zullen zijn.

Microsoft raadt dan ook aan om te streven naar een zo hoog mogelijk functional level.
Bij het opzetten van een nieuw forest brengt dat meestal geen problemen mee.
Bij een bestaand forest moet daarbij ook rekening gehouden worden met de serverversie die draait op de verschillende domeincontrollers.

Bij oudere versies geldt: eens overgeschakeld naar een hoger functional level, is terugkeren naar een lager niet meer mogelijk. Vanaf Windows Server 2008 R2 kan dat wel voor het domein functional level.

Bij de laatste versies werden relatief weinig nieuwigheden geïntroduceerd. Het verhogen van het functional level is daardoor niet altijd even interessant.

Een overzicht van de extra mogelijkheden per functional level vind je op

Active Directory Domain Services functional levels | Microsoft Learn

Specifiek voor Windows server 2016 hebben de nieuwigheden op domein functional level te maken met Kerberos authentication en Credential Protection. Op forest functional level gaat het om Privileged access management (PAM) using Microsoft Identity Manager (MIM)

Aan Windows Server 2019 en 2022 werd geen extra functional level toegevoegd.

Bij Windows Server 2025 heeft de nieuwigheid te maken met “Database 32k pages optional feature”.

## Authenticatie

Authenticatie betekent dat gebruikers moeten bewijzen dat ze wel degelijk zijn wie ze beweren te zijn.

Alle computers die lid zijn van een domein vertrouwen allemaal eenzelfde groep domeincontrollers om de authenticatie van gebruikers voor hen af te handelen.

### 1.7.1 Aanmelden

Authenticatie gebeurt aan de hand van de gebruikersnaam en het wachtwoord die een gebruiker intypt op een cliëntcomputer die deel uitmaakt van het domein.

De gebruikersnaam en het wachtwoord worden bezorgd bij de Winlogon service die ze op zijn beurt bezorgt bij de Local Security Authority (LSA).

De LSA past een hash toe op het wachtwoord van de gebruiker en verwijdert het oorspronkelijk ingetypte wachtwoord.

De LSA contacteert vervolgens de Security Support Provider (SSP). Windows Server ondersteunt twee SSP’s: Kerberos en NTLM. Voor Windows 2000 of nieuwere clients wordt automatisch Kerberos gekozen.

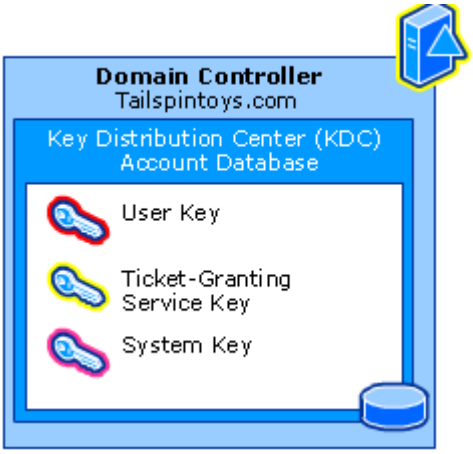
Een meer gedetailleerd overzicht vind je op

https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/windows-logon-scenarios

### 1.7.2 Kerberos

Kerberos ontleent zijn naam aan de hond met drie hoofden uit de Griekse mythologie. Bij authenticatie met het Kerberos protocol zijn er drie spelers:

- De client die de authenticatie vraagt
- De server die services aanbiedt waarvoor authenticatie nodig is
- Een computer die zowel door de client als door de server vertrouwd wordt, de KDC (Kerberos Key Distribution Center).




Kerberos verifieert zowel de identiteit van de gebruiker die zich aanmeldt als van de server die de authenticatie uitvoert. Dit gebeurt op basis van gedeelde sleutels.

Bij Windows Server is de domeincontroller meteen ook de KDC.

Bij het aanmaken van een gebruiker wordt een hashfunctie toegepast op het wachtwoord van die gebruiker. Het resultaat wordt opgeslagen als attribuut van de gebruiker in AD.

Op het ogenblik dat een computer lid wordt van het domein krijgt ook het systeem een wachtwoord. Op basis van dat wachtwoord wordt een systeemsleutel gegenereerd.

| Opmerking: Kerberos werkt met secret key versleuteling. Daarbij wordt niet zoals in public key versleuteling gewerkt met een sleutelpaar |
|---|

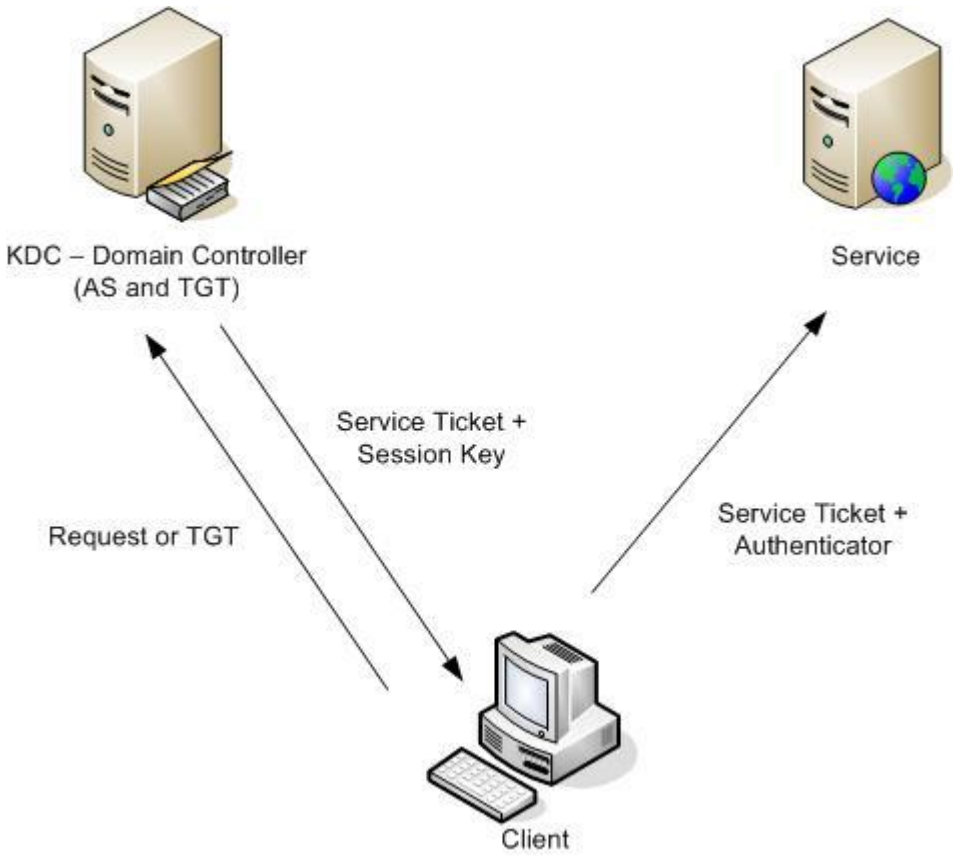
De authenticatie procedure verloopt dan als volgt:

1. De gebruiker meldt zich aan en de computer stuurt de gebruikersnaam naar de KDC, samen met de domeinnaam, een aanvraag voor een Ticket-granting Ticket (TGT) en preauthentication data waaronder een time stamp. De preauthentication data zijn geëncrypteerd met de sleutel van de gebruiker.

| Let op: de sleutel wordt niet meegestuurd over het netwerk! |
|---|

2. De domeincontroller zoekt de sleutel van de gebruiker aan de hand van de gebruikersnaam in AD DS. De DC ontcijfert aan de hand van deze sleutel de preauthentication data en controleert de timestamp. Als het ontcijferen lukt en de timestamp valt binnen de aanvaarde grenzen, dan bereidt de DC de authenticatie van de gebruiker voor. Als het ontcijferen mislukt of de timestamp valt niet binnen de vooropgezette grenzen, faalt de authenticatie.
3. In geval van succesvolle authenticatie creëert de KDC vervolgens twee items:
    - een sessie sleutel om te delen met de gebruiker, geëncrypteerd met de sleutel van de gebruiker
    - een Ticket Granting ticket (TGT; het TGT bevat ook een kopie van de sessie sleutel, de gebruikersnaam en een geldigheidstijdstip). De KDC encrypteert dit ticket met zijn eigen sleutel

    en bezorgt die bij de client.
4. Telkens de gebruiker vanaf nu een service nodig heeft, biedt hij zijn TGT aan bij de KDC versleuteld met zijn sessie key.




## 1.8 Roles and features

Een toestel met daarop als besturingssysteem Windows Server kan verschillende functies vervullen in een netwerk: domeincontroller, fileserver, printserver, DNS server, DHCP Server ....

Sinds Windows Server 2008 worden bijkomende **roles en features** geïnstalleerd per bijkomende functie die de server moet vervullen.

In andere modules worden de individuele rollen meer in detail besproken.

# 2 INSTALLATIE VAN WINDOWS SERVER

## 2.1 Harwarevereisten

Een overzicht van de hardwarevereisten vind je op https://docs.microsoft.com/en-us/windows-server/get-started/hardware-requirements .

Minimum vereisten samengevat:

| | Minimum | Aanbevolen |
|---|---|---|
| Processor | 1.4 GHz 64-bit processor | 3,1 GHz 64-bit processor |

Recente machines zullen ook voldoen aan de bijkomende vereisten:

- Compatible with x64 instruction set
- Supports NX and DEP
- Supports CMPXCHG16b, LAHF/SAHF, and PrefetchW
- Supports Second Level Address Translation (EPT or NPT)

🛠 Zoek de betekenis van deze termen op en vraag de eigenschappen van de CPU in je toestel op met *Coreinfo*. Vergelijk.

| | Minimum | Aanbevolen |
|---|---|---|
| RAM | 512 MB zonder grafische info<br>2 GB met Desktop Experience | 16 GB |

Bijkomende vereiste: ECC (Error Correcting Code).

🛠 Wat betekent ECC? Hoe kan je testen of het RAM geheugen van jouw computer van het type ECC is?

| | Minimum | Aanbevolen |
|---|---|---|
| Schijfruimte | min 32GB | 64GB |

Bijkomende vereisten:

Storage controller die voldoet aan de PCI Express architecture specificatie

| | |
|---|---|
| Ethernet adapter | Minstens 1 Gb throughput<br>Volgens de PCI Express architecture specificatie. |

Ondersteunt Pre-boot Execution Environment (PXE)

- Maak een virtuele machine die voldoet aan de systeemvereisten om Windows server te installeren. Kies voor een RAM geheugen van 4GB en een harde schijf van 80 GB.

## 2.2 Installatie van het serverbesturingssysteem

Om een testtoestel te installeren kan je een evaluatie iso van het besturingssysteem downloaden van de Microsoft site.

Installeren kan o.a. van een bootable USB of van een DVD.

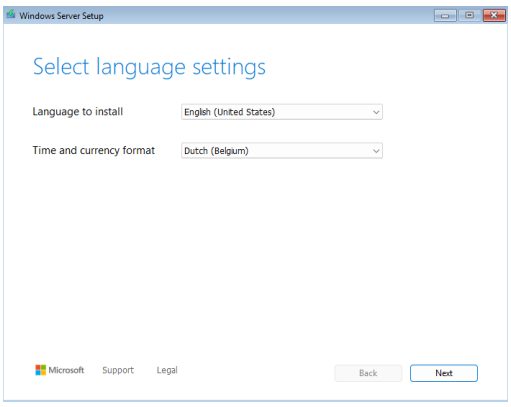
- Haal het ISO-bestand op van Microsoft Evalation Center met een evaluatie versie van het Windows server besturingssysteem.

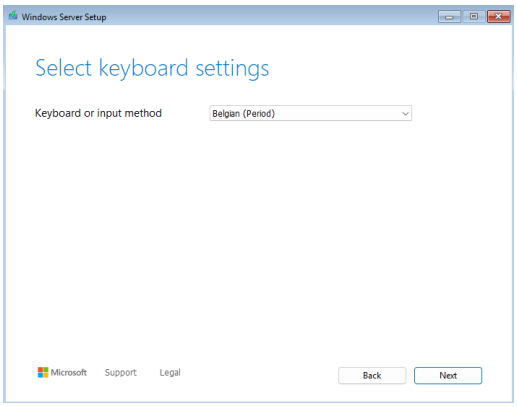
- Koppel de ISO aan de DVD van de virtuele machine en start de machine. De installatie van het besturingssysteem wordt opgestart.

Een wizard maakt de installatieprocedure eenvoudig en gebruiksvriendelijk.

Enkele aandachtspunten tijdens de installatie:

- Zorg voor de juiste formaat voor tijd en munt, plus ook het juiste het toetsenbord




In ons geval:

- Time and currency format: **Dutch (Belgian)**
- Keyboard or input method: **Belgian (Period)**

- Setup option:

  Kies voor “**Install Windows Server** “

  Zet een vnkje voor “**I agree …**”

- Keuze van de editie van het besturingssysteem

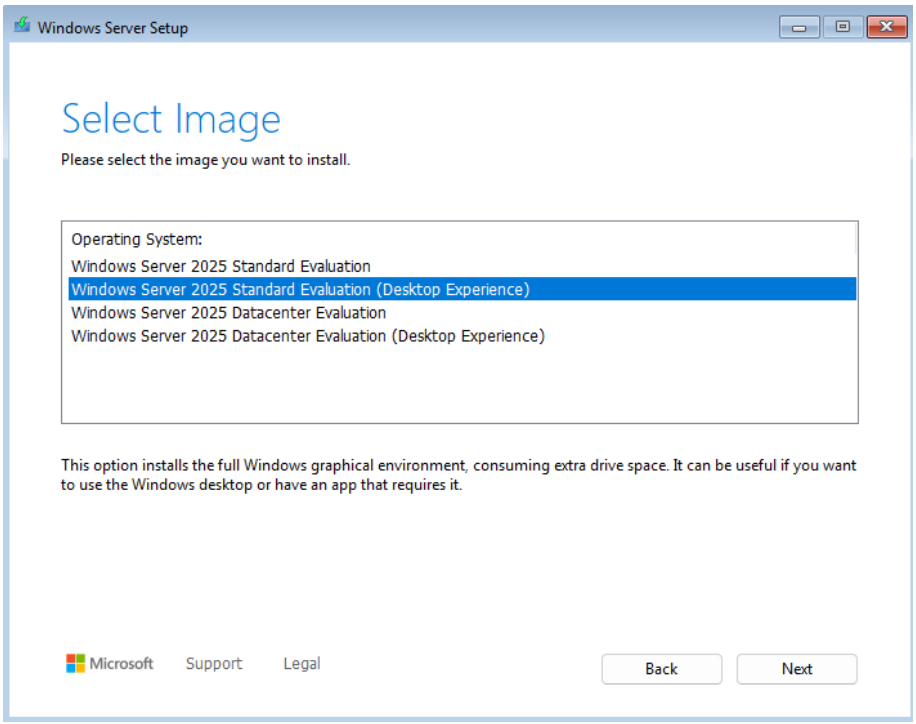
De eerste optie, Standard, komt overeen met een installatie zonder grafische interface. Indien je een grafische interface wil gebruiken, kies dan de tweede optie (**Desktop experience**).

Standaard versus datacenter

Het verschil tussen deze twee edities heeft o.a. te maken met licenties voor virtuele machines. In de standaard editie is een licentie voor 1 Hyper-V host en twee virtuele machines begrepen, in de datacenter editie is dat een onbeperkt aantal virtuele machines.

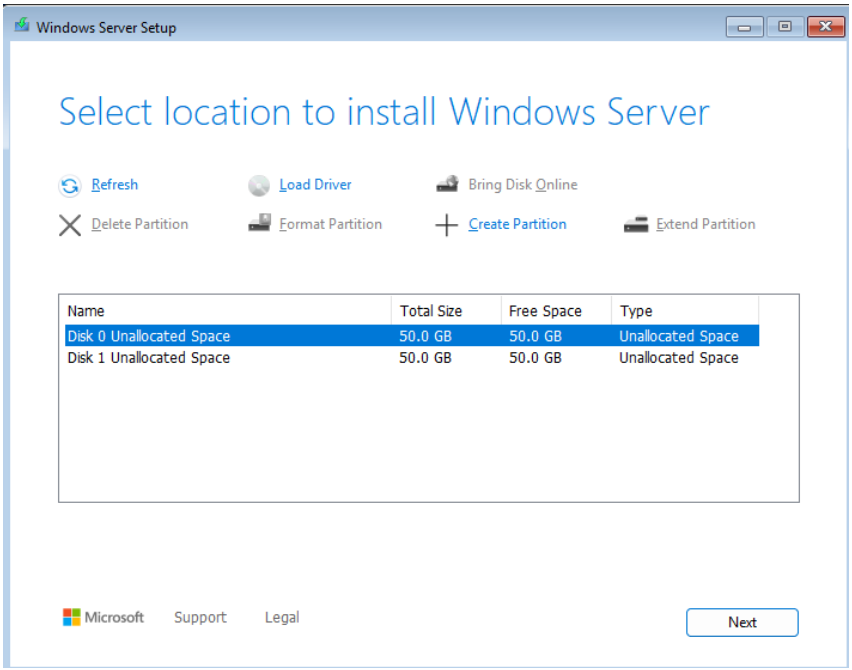
De datacenter editie ondersteunt, in tegenstelling tot de standaardeditie ook storage replica, software-defined networking en storage spaces direct.

Een volledig overzicht van de verschillen vind je op https://learn.microsoft.com/en-us/windows-server/get-started/editions-comparison?pivots=windows-server-2025

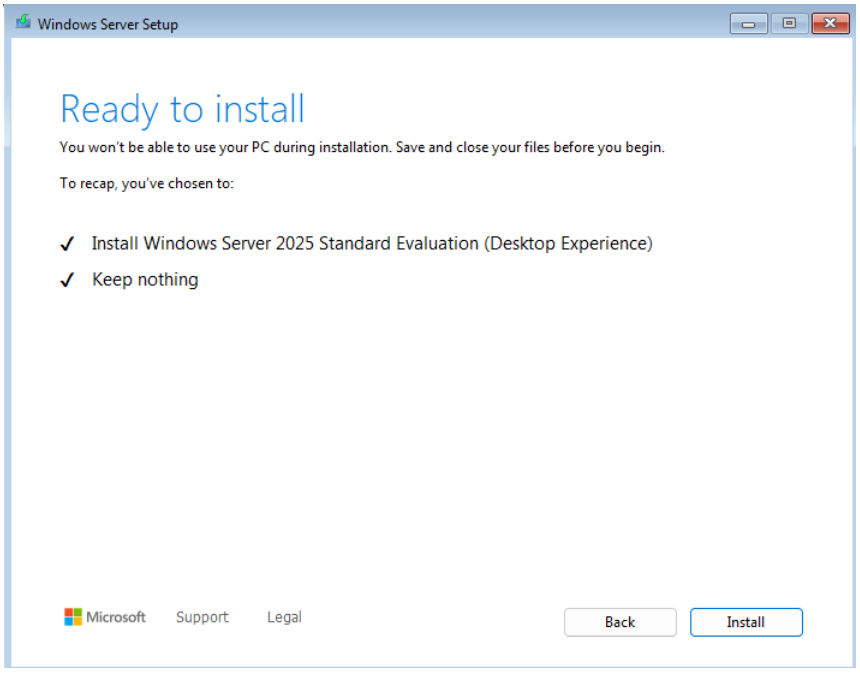



- Kies voor het doornemen van deze module de **standaardeditie met desktop experience**, maw de **tweede** optie.
- Accepteer de licentie voorwaarden.
- Kies de schijf waarop de installatie moet gedaan worden

**Good practice: installeer besturingssysteem en data op aparte partities of op aparte schijven!**




De Windows installatie procedure heeft nu voldoende informatie om de installatie uit te voeren.

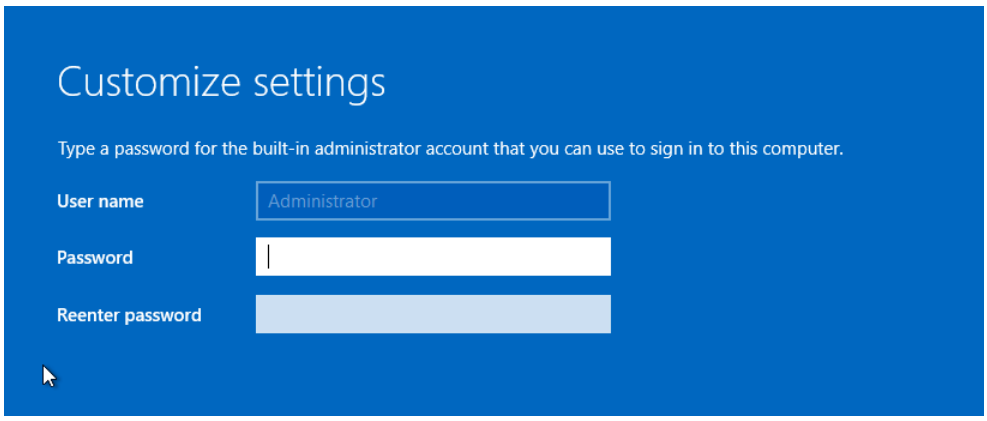



🛠 Druk op **Install** om de installatie te starten

Het merendeel van de tijd van de installatieprocedure wordt in beslag genomen door de fase **Copying en Expanding Windows files.**

Nadien herstart de server om **de rest van de installatie** te voltooien. De kans bestaat dat meerdere keren herstarten nodig is. Je hoeft zelf niets te doen, dat gebeurt automatisch.

🛠 Ten slotte verschijnt de vraag naar een wachtwoord voor de administrator.



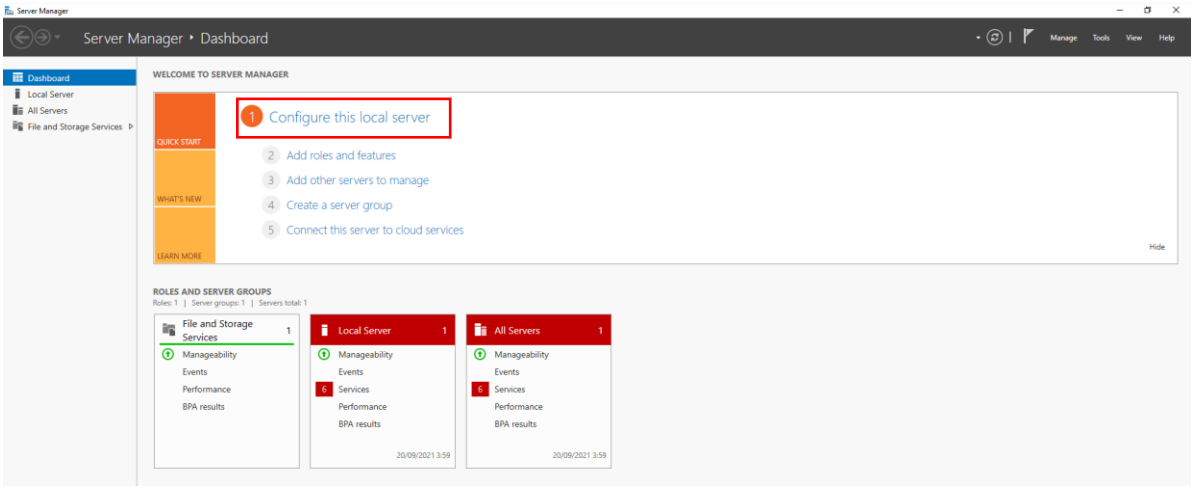

Hou rekening met de complexity vereisten voor wachtwoorden. Dit is standaard geactiveerd voor Server 2025 en betekent dat

- wachtwoorden minstens 7 karakters lang moeten zijn
- van de vier karakterverzamelingen (hoofdletters, kleine letters, cijfers en speciale karakters) er minsten drie moeten vertegenwoordigd zijn.

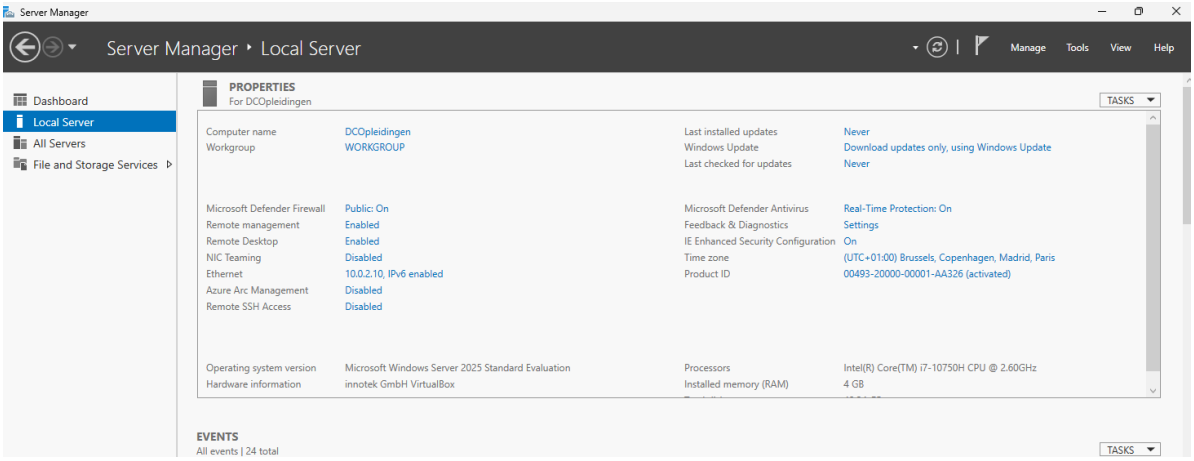
De installatie is voltooid.

# 3 INITIËLE CONFIGURATIE NA INSTALLATIE

Op het einde van de installatie wordt na het aanmelden, automatisch de Server Manager opgestart en het Dashboard verschijnt.




**Configure this local Server** geeft een overzicht van en links naar alle instellingen die al meteen een correcte configuratie vereisen.




## 3.1 De computernaam

Tijdens de installatie heeft de server al een naam gekregen. Deze naam zal uniek zijn op het netwerk, maar bevat verder geen informatie en is moeilijk te onthouden. Omdat er b.v. bij het delen van mappen enz. zal verwezen worden naar de naam, kan het toch belangrijk zijn om even stil te staan bij de naamgeving.

Enkele suggesties

| Suggestie | Bedenk zelf in welke omgeving deze suggestie een voor- of een nadeel kan zijn |
|---|---|
| Maak alle computernamen even | Gemakkelijk te ontleden, nuttig bij automatisatie b.v. via scripts |

| | |
|---|---|
| lang en stel ze op dezelfde manier samen | |
| Rol van de computer | Het is gemakkelijk te identificeren welke functie op het netwerk de computer vervult |
| Verwijzing naar het platform (OS) | Alleen nuttig in een omgeving waarin met verschillende besturingssystemen gewerkt wordt |
| Locatie | De computer is gemakkelijk terug te vinden, nadeel: de naam moet aangepast worden bij verplaatsing van de computer |
| Naam van de gebruiker | Een gegeven dat nogal eens verandert en een potentieel risico voor de veiligheid |

Inspiratie kan je o.a. opdoen op onderstaande website

https://www.techrepublic.com/article/determining-a-good-naming-convention-for-your-network/

🛠 Geef je server de naam **DCopleidingen**.

## 3.2 Het domein

Onmiddellijk na installatie is de server lid van een werkgroep. Er zijn nu een aantal mogelijkheden

- De server wordt lid van een bestaand domein, een memberserver
- De server wordt domeincontroller van een nieuw domein
- De server wordt tweede domeincontroller van een bestaand domein

Voorlopig behouden we werkgroep.

## 3.3 Windows Firewall

Is de Firewall ja dan nee geactiveerd. De link brengt je naar de instellingen van de Firewall.

## 3.4 Remote management

Om beveiligingredenen staan servers meestal in een serverkamer (voorzien van airco) en/of in een serverkast. De administrator zal zelden tot in de serverkamer lopen om de server te configureren of te raadplegen. Servers worden in vele gevallen vanop afstand/remote aangesproken. Dit kan alleen als de server deze remote connectie aanvaardt. De link geeft je de optie om Remote management in of uit te schakelen.

Het besturingssysteem beschikt over meerdere ingebouwde tools om een server vanop afstand te beheren:

- PowerShell
- Server Manager
- Mmc's
- Remote desktop
- Remote SSH access

Microsoft raadt PowerShell aan.

🛠 Schakel indien nodig remote management in.

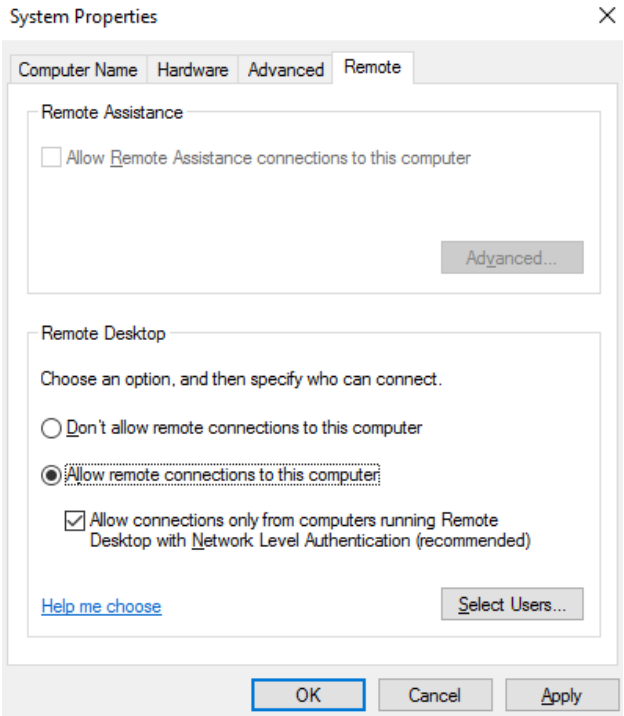
## 3.5 Remote desktop

Deze link opent het **tabblad Remote** van de **System properties**.

Standaard worden remote connections niet toegelaten.

Zodra je remote connections wel toelaat kan je nog bijkomend eisen dat dit alleen mag via clients die Network Level Authentication ondersteunen. De RDP server luistert standaard op TCP poort 3389. Deze poort wordt ook geopend in de FW bij het activeren van remote desktop connections.

Via de knop **Select Users** kan je nog bepalen welke gebruikers een remote connection met de server mogen opzetten. Standaard hebben alleen administrators dat recht.




De rol van Network Level Authentication (NLA)?

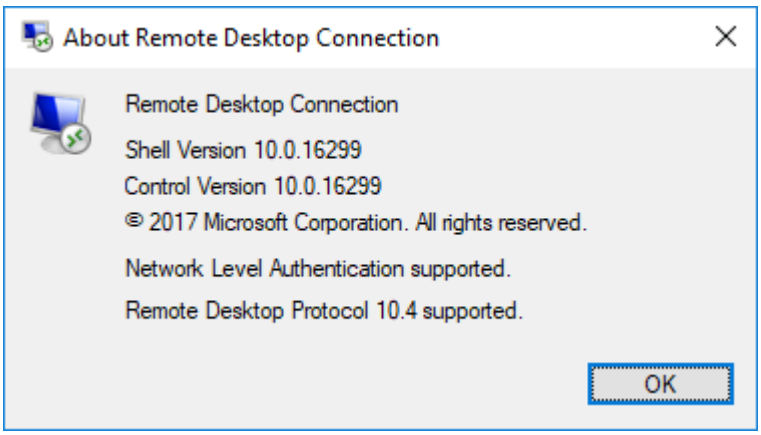
Dit is de meest veilige manier om een remote desktop connectie toe te laten op de server. NLA forceert de client computer om een authenticatie aan de gebruiker te vragen alvorens een remote sessie wordt opgezet voor die gebruiker.

Vanaf Windows Vista met SP1 is Remote Desktop Connection uitgerust met Network Level Authentication.

Hoe controleer je of jouw remote desktop client NLA ondersteunt?

🛠 Start het programma **Remote Desktop Connection** op de client

🛠 Klik op het icoontje links in de titelbalk en kies **About**




Hier zie je de versie van Remote Desktop Connection die op je toestel geïnstalleerd is en of deze versie Network Level Authentication ondersteunt.

## 3.6 NIC teaming

NIC teaming laat toe om (max 32) fysieke Ethernet netwerk adapters te groeperen tot één virtuele netwerk adapter. Dit maakt hogere transportsnelheden en fouttolerantie mogelijk.

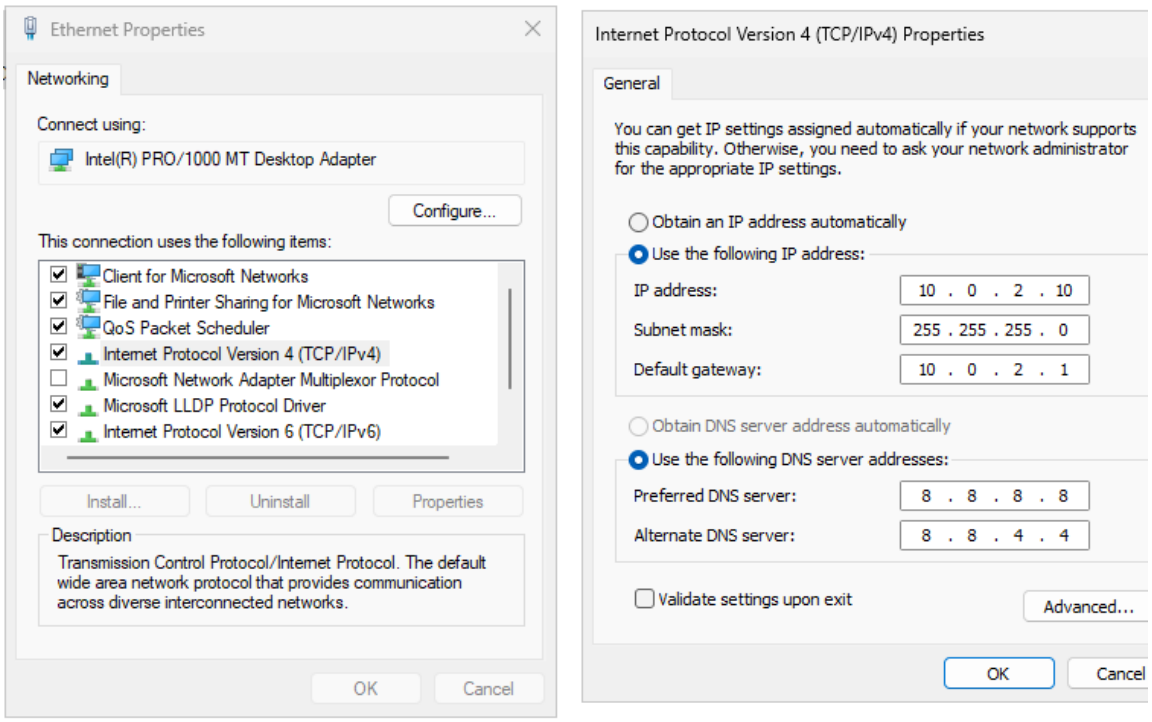
## 3.7 Ethernet

Brengt je naar het dialoogvenster Network Connections van waaruit je de netwerkinstellingen kunt configureren.

Servers krijgen in een netwerk altijd een statisch IP adres. Via **Local Area Connection** stel je een vast IP adres in samen met de andere TCP/IP instellingen zoals subnetmask, default gateway, DNS, enz…

- Klik met de rechtermuisknop op het icoon van de **Ethernet** en kies **properties**.
- Selecteer **Internet Protocol Version 4** en klik op de knop **properties**
- Selecteer **Use the following IP address** en vul de IP adressen in.

**De IP adressen in de figuur zijn enkel als voorbeeld bedoeld, bespreek met je instructeur welke IP adressen je kan en mag gebruiken!**




Als zowel IPv4 als IPv6 ingeschakeld zijn, dan zal Windows Server een verbinding altijd eerst via IPv6 proberen te maken.

Afhankelijk van de manier waarop je de netwerkverbinding binnen je labo organiseert zal je dus ook vaste IPv6 adressen moeten voorzien.

## 3.8 Updates

Dit deel van het venster toont wanneer de updates de laatste keer gecheckt en doorgevoerd werden. De link brengt je naar de instellingen voor updates.

Net zoals bij Windows 10 gebeuren de updates bij Windows Server vanaf versie 2016 volledig automatisch, zonder tussenkomst van de beheerder. Het tijdstip waarop een server herstart na een update is wel configureerbaar.

**Opmerking**: In veel gevallen is in het netwerk ook een WSUS server voorzien. WSUS staat voor Windows Server Update Services. Deze server verzorgt het downloaden van de updates en het verspreiden ervan binnen het netwerk. Group Policies zorgen dan voor de juiste configuratie. WSUS is onderwerp van een aparte module.

- 🛠 Ga na of je server volledig up to date is. Zo niet, installeer dan de de laatste updates.

## 3.9 Windows Defender

Toont de toestand en brengt je naar de instellingen van Windows Defender.

## 3.10 Feedback & Diagnostics

Hier configureer je welke informatie doorgespeeld wordt naar Microsoft.

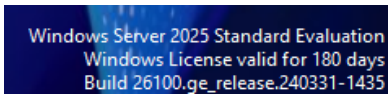
## 3.11 Time zone

Spreekt voor zich. Zorg ervoor dat je de juiste tijdzone ingesteld hebt indien dit niet het geval is.

## 3.12 Product ID

Heb je bij het installeren nog geen product key ingegeven dan kan je dit alsnog via deze link doen. Na het ingeven van de product key kan er geactiveerd worden.

Indien je een evaluatieversie hebt gebruikt voor de installatie, zal deze automatisch ingevuld staan.  Je kan dan deze installatie gebruiken gedurende 180 dagen.




*Alvorens verder te gaan controleer je zeker dat je volgende zaken correct het geconfigureerd:*

- *Computer Name*
- *Remote Desktop*
- *Ethernet*
- *Windows Update*
- *Time zone*
- *Product ID*

Indien nodig, herstart je de server.

# 4 EEN DOMEINCONTROLLER INSTALLEREN

Na de basisinstallatie van de server volgt de verdere configuratie in functie van de rol van de server.

Een eerste server op een netwerk zal (bijna altijd) een domeincontroller worden.

De installatie van Active Directory Domain Services op een Windows Server besturingssysteem is dankzij de AD DS Wizard vrij eenvoudig.

Na installatie van AD DS is de server een Domain Controller. De stand-alone server is als het ware gepromoveerd naar een Domain Controller (DC). Het commando om deze promotie tot stand te brengen (dus de installatie van AD DS) draagt dan ook de naam DCPROMO.EXE.

🛠 Controleer nog even of je machine aan de systeemvereisten voor een DC voldoet:

- Een harde schijf van minimum 10 GB, 40 GB en meer zijn aanbevolen
- Een statisch (vast) IP adres

Zelf moet je de nodige administratieve rechten hebben.

## 4.1 De rol van DNS

### 4.1.1 Het belang van DNS

Op het Internet beantwoordt DNS vragen zoals welk IP-adres is gekoppeld aan www.vdab.be?

Sinds Windows Server 2000 gebruikt AD DNS ook voor de omzetting van Namen naar IP-adressen op het interne netwerk. Je kunt geen AD installeren zonder DNS.

Voor naamomzettingen op het Internet registreert een bedrijf twee (fouttolerantie) DNS servers via zijn provider. Uitleg hieromtrent valt buiten het bestek van de cursus.

Op het interne netwerk is er in functie van AD minimaal één DNS server nodig. Ook in deze context zijn twee servers wenselijk omwille van fouttolerantie. Het is in de praktijk een goed idee om de gekozen DNS-naam voor het interne netwerk verschillend te kiezen van de internetnaam.

Opmerking

Microsoft raadt aan voor de interne domeinnaam te werken met subdomeinen. Dit sluit aan bij de richtlijnen van RFC 2606.

In een labo omgeving vertaalt dat zich in een aantal opties voor de domeinnamen:

Ofwel gebruik je

- .test
- .example
- .invalid
- .localhost

als suffix

ofwel gebruik je example als second level domeinnaam zoals in

- example.com
- example.net
- example.org

DNS slaat zijn informatie op in de vorm van records georganiseerd in zones. Het type van een record bepaalt welke informatie dat record opslaat.

### 4.1.2 Enkele types van DNS-record

In functie van naamomzettingen vind je o.a.

A-records

Dit is het meest voorkomende type record. Het verbindt een naam aan een Ipv4 adres, b.v. de naam vdab.be aan het IP-adres 193.53.101.103

AAAA-records

Koppelen ook een naam aan een IP-adres, maar dan een IPv6 adres.

SOA-records

Een van de belangrijkste records. SOA staat voor Start Of Authority. Hiermee wordt een onderscheid gemaakt tussen een primary zone en een secondary zone. Er wordt een email adres gemaakt voor de administrator, caching wordt ingesteld. En het communiceert met de buitenwereld bij wijzigingen aan de DNS.

Cname-records

Vaak zal een toestel verschillende taken hebben bv een ftp- en een http-server, deze wil je dan onderscheiden met verschillende namen bv ftp.vdab.be en www.vdab.be. Beide verwijzen wel naar hetzelfde adres 193.53.101.103. Hiervoor maken we dan een alias of een Cname-record.

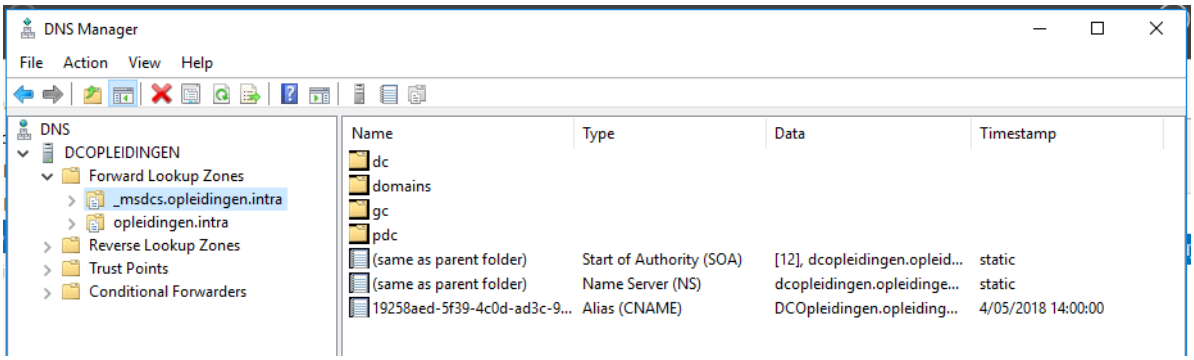
MX-records

Bij het versturen van een mail naar b.v. bpeeters@vdab.be, is de naam van de mailserver niet gekend. De mail wordt verstuurd naar het domein vdab.be. Het MX record bepaalt dan waar de mailserver voor dat domein zich bevindt.

Hoe DNS juist aan het werk gaat om een naam om te zetten naar een IP-adres wordt gedetailleerd toegelicht in de appendix op het einde van dit document.

In een domeinomgeving creëert dcpromo.exe (de installatiesoftware voor een DC) naast deze records ook service records in DNS.

Clients op het domein gebruiken servicerecords om te ontdekken via welk toestel bepaalde services aangeboden worden. Zo vindt een client via de service records niet alleen een domein controller om zich bij aan te melden, maar ook op welke server(s) een global catalog, de pdc, .. te vinden zijn.



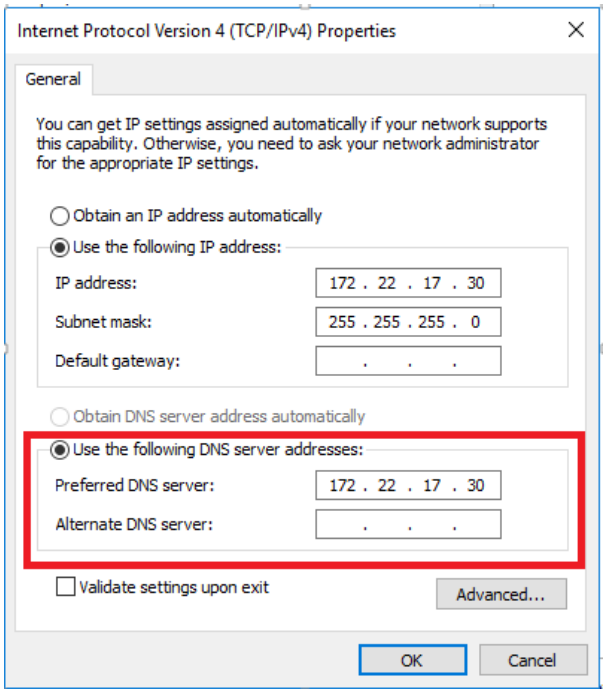

### 4.1.3 DNS installeren

De eenvoudigste manier van werken is DNS meteen samen met AD DS installeren.

### 4.1.4 De DNS server kenbaar maken

Zowel op de server als op de client toestellen moet duidelijk gemaakt worden op welk toestel de DNS service te vinden is.

Dit gebeurt bij de IP-instellingen van het toestel.



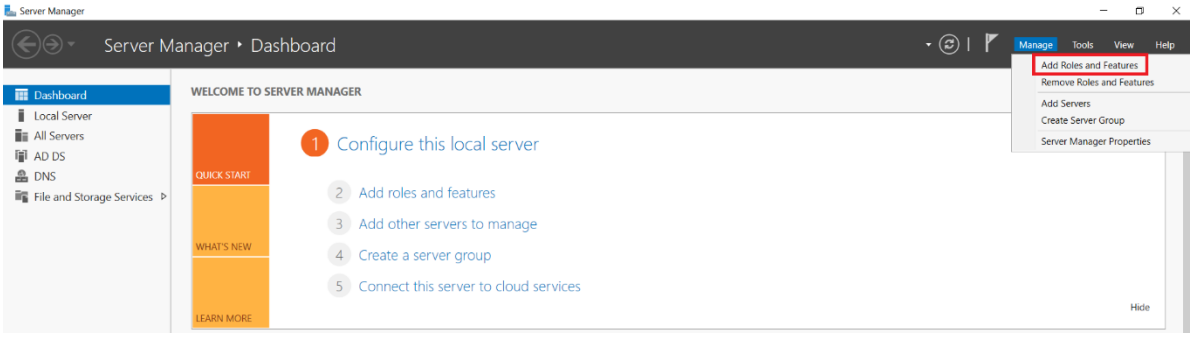
## 4.2 Installatie van Active Directory Domain Services in de praktijk

De installatie van Active Directory Domain Services verloopt in twee stappen

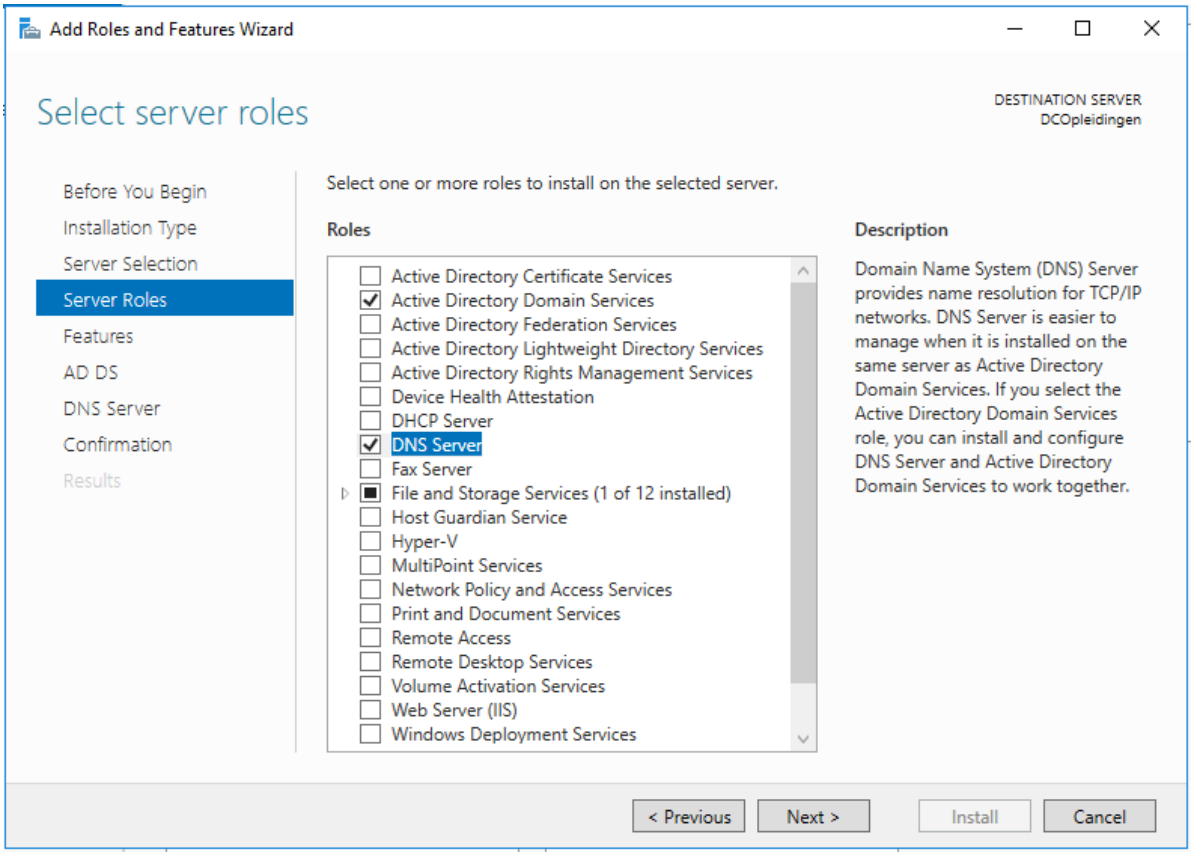
1. Installatie van de AD DS Role via de Server Manager
2. Verdere configuratie met de AD DS installation Wizard door het uitvoeren van DCPROMO

### 4.2.1 Installatie van de AD DS Role

- Open de **Server Manager** en ga naar het **Dashboard**




- Klik op **Add Roles and features**. De **Add Roles and Features Wizard** start
- **Select Installation type**: kies **Role based or feature based installation**
- **Select destination server:** kies **Select a server from the server pool** en selecteer de server
- **Select server roles:** Vink **Active Directory Domain Services** en **DNS server** aan. Klik voor beide ook op **Add Features** om meteen ook alle noodzakelijke bijkomende features te installeren.




- **Select Features:** klik meteen op Next. Er is al gevraagd om alle nodige bijkomende features te installeren.

De volgende stappen geven nog wat extra uitleg bij **AD DS** en **DNS** en ten slotte volgt **Confirmation**, een samenvatting van de gevraagde instellingen.

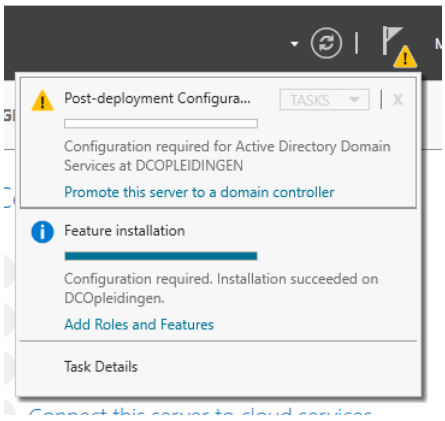
- Klik op Install om de installatie te starten.

**Results** toont hopelijk dat de installatie gelukt is, maar meldt meteen dat je nog een DCPROMO dient uit te voeren om van de server een volwaardige Domain Controller te maken.

- Ook de Server Manager geeft aan dat AD DS geïnstalleerd is, maar dat DCPROMO nog dient uitgevoerd te worden.

### 4.2.2 DCPROMO

🛠 Klik op het waarschuwingsteken en dan op de link **Promote this server to a domain controller** om dcpromo, de AD DS Configuration wizard, op te starten.



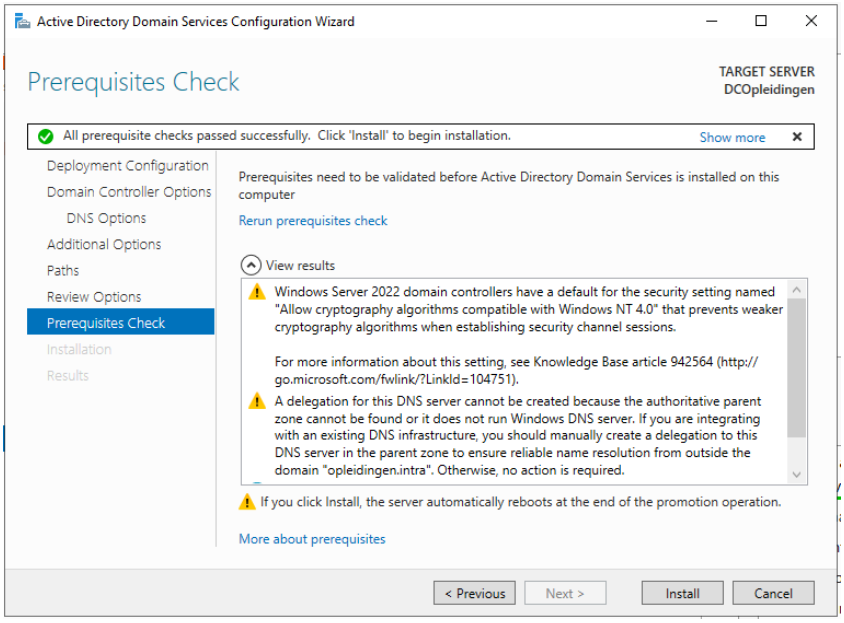

**Deployment configuration** biedt drie opties voor de domein controller:

| | |
|---|---|
| Add a domain controller to an existing domain | De nieuwe domein controller wordt lid van een bestaand domein en zal de inhoud van zijn AD synchroniseren met die van de al bestaande domeincontroller. |
| Add a new domain to an existing forest | Het is de bedoeling een child domein of een nieuwe tree te maken binnen het bestaande forest. |
| Add a new forest | Dit is de eerste domein controller van het eerste domein binnen het forest. |

Het vervolg van deze uitleg gaat uit van de derde keuze, de domein controller is bestemd voor het eerste domein van een nieuw forest. De naam van het domein wordt **opleidingen.intra**.

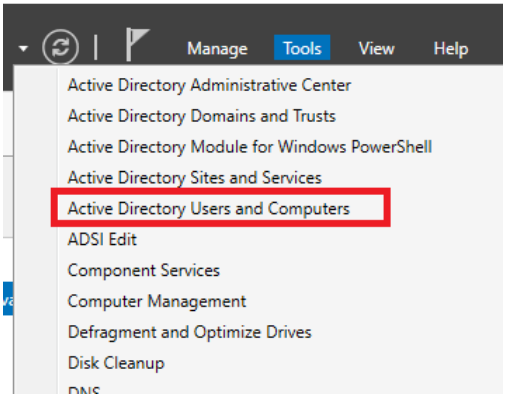
De wizard zal nu verdere configuratie informatie opvragen via een aantal schermen:

| | |
|---|---|
| Domain controller Options | Het **functional level** voor forest en domein worden standaard op **2025** gezet. Aangezien we een nieuw forest opzetten, behouden we deze instellingen.<br><br>Best practice is om op elke domein controller ook de DNS service en een Global Catalog te installeren.<br><br>Het DSRM wachtwoord is het wachtwoord dat zal gebruikt worden als er problemen zijn met de domein controller en die niet op een normale manier kan opgestart worden. Het staat los van het wachtwoord van de administrator. |
| DNS Options | Er verschijnt een waarschuwing: |

| | |
|---|---|
| | **A delegation for this DNS server cannot be created because the authoritative zone cannot be found**<br><br>Dit verwijst naar een zone intra die niet gevonden wordt op de DNS server.<br><br>Je mag deze melding negeren en verder gaan met de volgende stap. |
| Additional Options | De installatie stelt zelf een NetBIOS naam voor. Dit kan even duren aangezien er moet onderzocht worden of OPLEIDINGEN (eerste deel van je domeinnaam) kan gebruikt worden. |
| Paths | Waar worden de AD Database, log files en sysvol folder opgeslagen?<br><br>Je behoudt hier het voorgestelde pad. |
| Review Options | Een samenvatting van de gemaakte keuzes. |
| Prerequisites Check |  <br>Er verschijnen een aantal aandachtspunten. Belangrijk is de melding bovenaan. |
| Result | Het resultaat van de installatie. In geval van succes wordt de server automatisch herstart. |

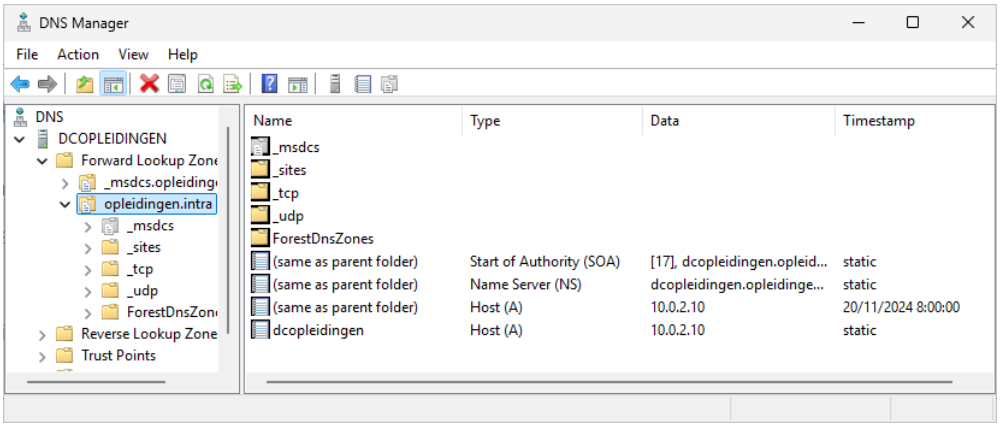
### 4.2.3 Controle van de installatie

**Active Directory Users and Computers** en **DNS** werden, samen met andere tools om AD DS te beheren, toegevoegd aan de Tools in de Server Manager.



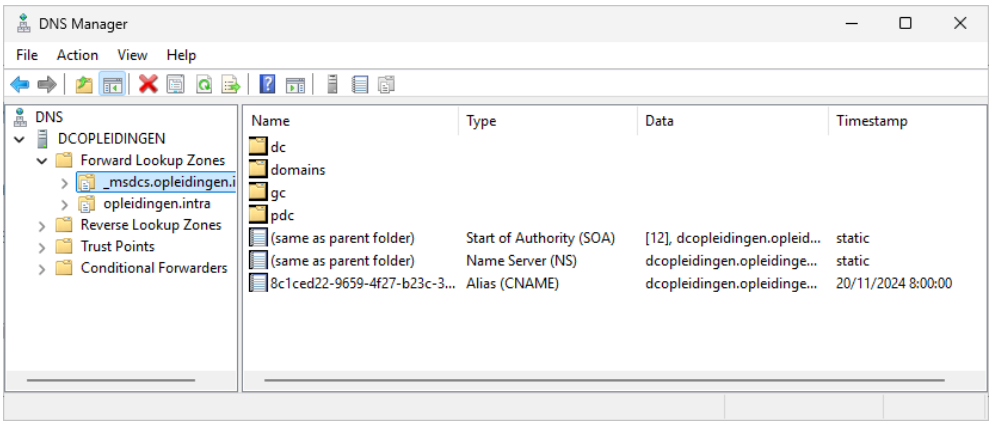

De map sysvol werd aangemaakt: c:\Windows\sysvol

In DNS is een zone aangemaakt met de naam van het domein. Hieronder zullen de omzettingen voor toestellen in het domein te vinden zijn.



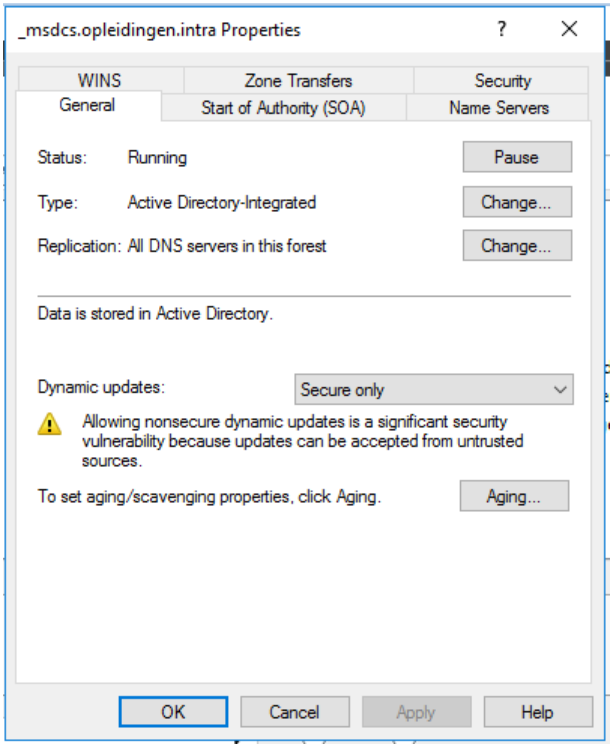

**Opmerking**

De _msdcs.opleidingen.intra zone wordt enkel aangemaakt als je DNS installeert samen met de AD DS (via DCPROMO).




Om goed samen te werken met AD DS moet de configuratie van DNS aan bepaalde voorwaarden voldoen:

- Roep via de rechtermuisknop de eigenschappen op van de zone die overeenkomt met het domein.




Belangrijke instellingen:

Type: Active Directory –Integrated

De inhoud van de DNS zone is opgeslagen in AD en wordt als deel van AD met AD mee gerepliceerd.

Dynamic Updates: Secure only:

Alleen authenticated Active directory accounts en processen kunnen DNS resource records updaten.

## 4.3 Clients lid maken van het domein

Het clientbesturingssysteem dat optimaal gebruik maakt van de functionaliteiten van Windows Server 2025 is uiteraard Windows 11, maar ook clients met een oudere versie van het besturingssysteem kunnen lid gemaakt worden van het domein.

- 🛠 Installeer een client
- 🛠 Geef de client beschrijvende computernaam, b.v. CL01

De client moet eerst de juiste TCP/IP instellingen meekrijgen: een IP-adres binnen de range van het netwerk, een correct subnetmask, een default gateway en een verwijzing naar de DNS server om met naamresolutie overweg te kunnen en servicerecords op het domein terug te vinden.

De TCP/IP instellingen kunnen statisch (manueel) of dynamisch (met behulp van een DHCP server ingesteld worden.

### 4.3.1 Een client met statische IP-instellingen

**Ook hier zijn de in de afbeeldingen gebruikte IP-instellingen uitsluitend als voorbeeld bedoeld en overleg je bij twijfel best eerst met je instructeur of netwerkbeheerder!**

- Geef de client een IP-adres in hetzelfde subnet als de domeincontroller. Vul ook subnetmasker, default gateway en de DNS server in. Voor de DNS server verwijs je naar een toestel waarop je de rol van DNS server voor het domein geïnstalleerd hebt. Dus het IP-adres van je domain controller.

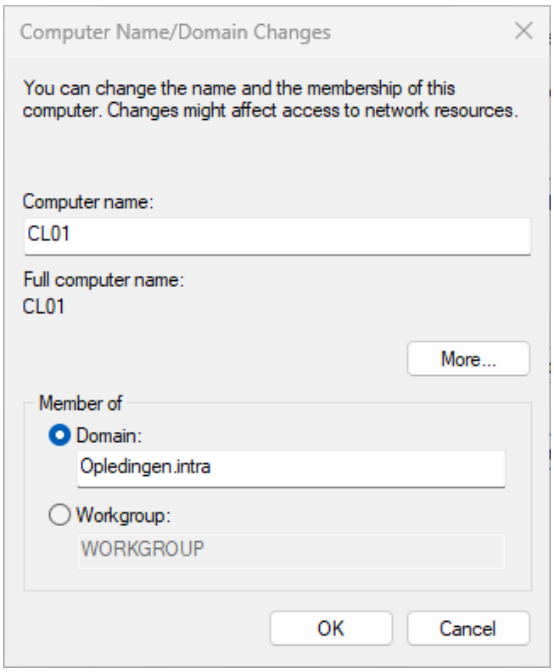
Lid maken van het domein gebeurt via de Systeem eigenschappen.

Windows 10:

- Ga naar Settings > System > About en maak de client lid van het domein via **Rename this PC (advanced)**.
- Dit brengt je naar het venster Computer Name / Domain Changes

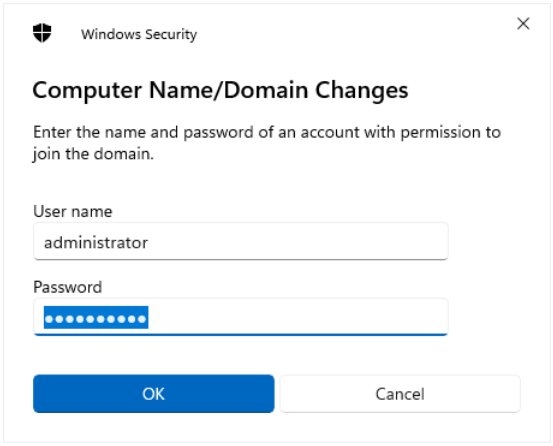
Windows 11:

- Ga naar Settings > System > About en maak de client lid van het domein via **Domain or Workgroup**.
- Op het scherm “System properties”, tabblad “Computer Name” klik je op de knop **Change**.
- Dit brengt je naar het venster Computer Name / Domain Changes




- Na het invullen van de domeinnaam druk je op OK

- Als alles goed gaat wordt de naam en het paswoord gevraagd van een gebruiker die het recht heeft om een toestel toe te voegen aan het domein. Aangezien we nog maar 1 gebruiker hebben in het domein, vul je daar als gebruiker “administrator” in samen met het paswoord.




- Op het einde zal je de computer moeten herstaren.

Van zodra de client lid is van een domein kan je op de client niet meer alleen met een lokale account aanmelden, maar ook met een domeinaccount. Om lokaal aan te melden op het toestel typ je **computernaam\username** of **.\username** als gebruikersnaam.

### 4.3.2 Een client met dynamische IP-instellingen

Manueel IP instellingen configureren op één enkele client gaat vlot. Honderden clients manueel configureren is saai werk en kan gemakkelijk aanleiding geven tot het maken van fouten. Een DHCP (Dynamic Host Configuration Protocol) server kan dit overnemen.

**De werking van een DHCP server kwam ook al aan bod in de module netwerken (CCNA2). Belangrijk is je te realiseren dat bij de communicatie tussen DHCP servers en clients broadcasts te pas komen. Bij de installatie van een DHCP server op je domein is het dan ook essentieel dat je erop let dat het broadcast domein van het labo en het broadcast domein van het netwerk thuis of in het centrum strikt gescheiden zijn.**

De rol van DHCP server kan niet alleen door een Windows server in het domein opgenomen worden, maar b.v. ook door een router of een Linux server.

In deze module gaat het erom dat een Windows Server de rol van DHCP server op zich neemt.

De rol van DHCP server wordt hier op hetzelfde toestel geïnstalleerd dat ook al dienst doet als domeincontroller en DNS server. In de praktijk kan je daarvoor ook een ander toestel in het domein kiezen.

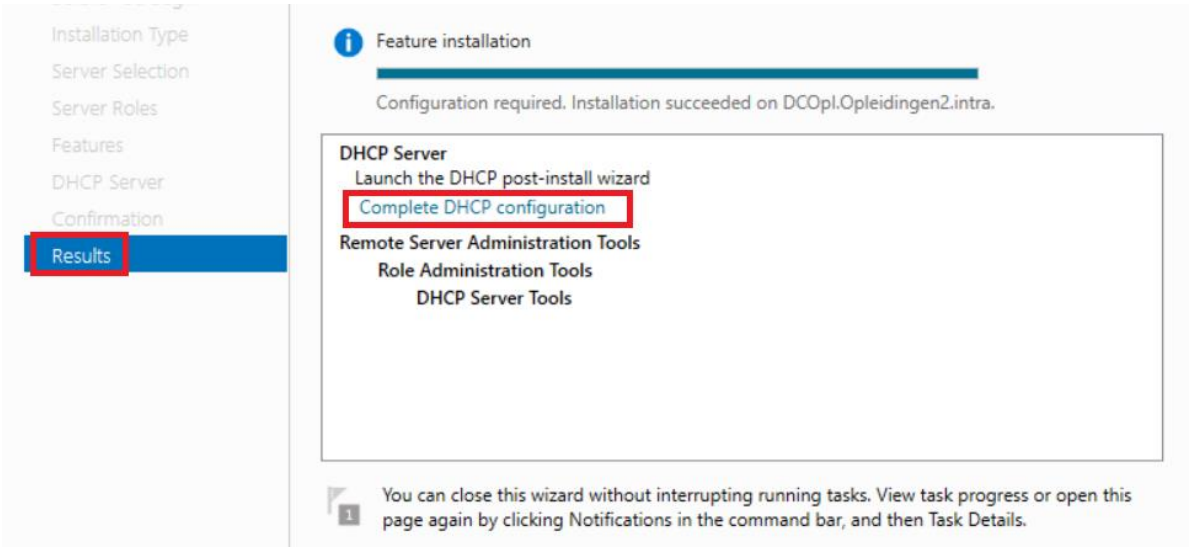
In Server Manager

- Manage > Add Roles and Features

- Select Installation type: **Role based or feature based installation**
- Select destination server: **Select a server from the server pool** en selecteer de server
- Select server roles: Vinkje bij **DHCP**
- Installeer meteen ook de managementtools (Add Features).
- Klik **Next** totdat je bij de fase **Results** van de wizard beland bent.

De DHCP rol wordt niet automatisch onmiddellijk geactiveerd. Dit heeft te maken met de problemen die zich op een netwerk kunnen voordoen als er twee (of meer) DHCP servers met tegenstrijdige configuraties op bestaan.

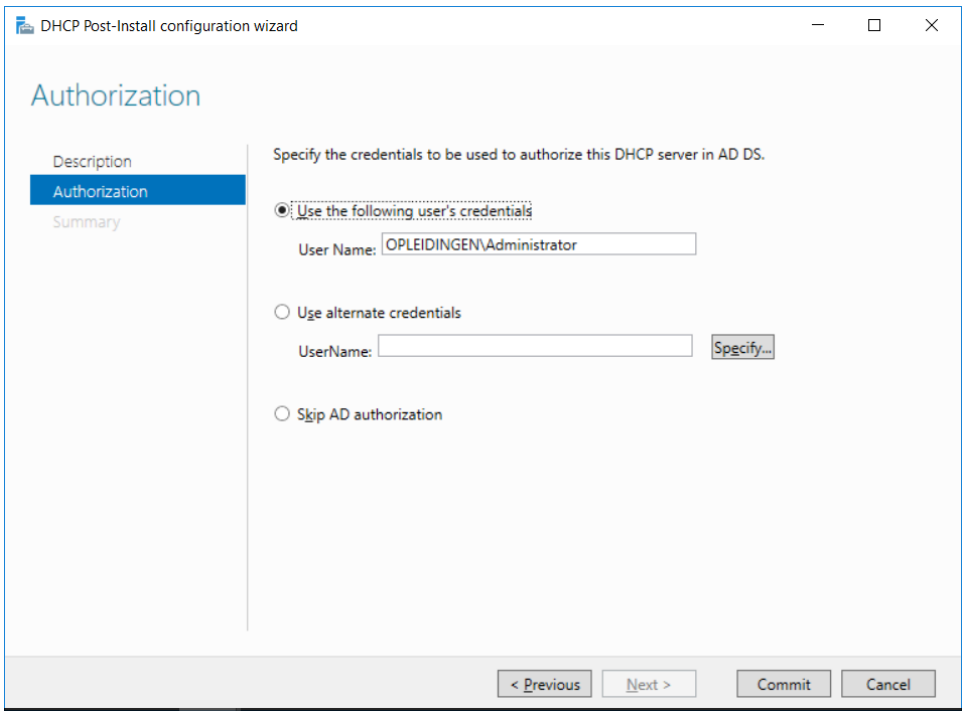
Op het einde van de installatie (fase Results) verschijnt daarom een link **Complete DHCP configuration** in het dialoogvenster.




Die kan een beheerder gebruiken om de DHCP server expliciet te activeren (authorize the DHCP server) alvorens die IP instellingen kan uitdelen.

Bij grote netwerken worden de verantwoordelijkheden bovendien dikwijls verdeeld over meerdere personen. Tijdens de Authorization kan daarom ook nog opgegeven worden wie de DHCP server zal beheren.

- Klik op de link **Complete DHCP configuration.**
- Klik op **Next** in de beschrijving en duid aan wie verantwoordelijk is voor de authorisatie van de server. In onze omgeving duiden we de domeinadministrator aan.




🛠 Klik op **Commit** om de installatie te beëindigen.

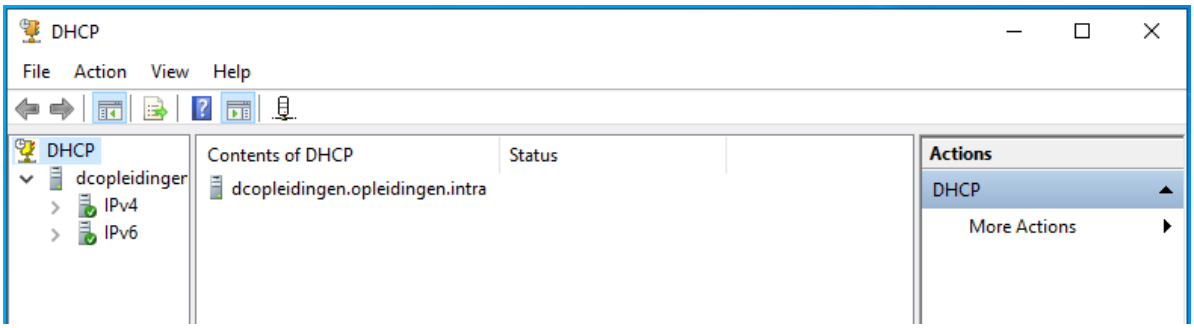
Tip:

DHCP kan ook met een PowerShell opdracht op een Windows Server geïnstalleerd worden:

```
Install-WindowsFeature DHCP -IncludeManagementTools
```

De DHCP server verder configureren

🛠 Roep de DHCP console op via **Server Manager > Tools > DHCP**




Tip:

De groene vinkjes bij IPv4 en IPv6 wijzen op de activatie van de DHCP server. Heb je de link **Complete DHCP configuration** in de vorige stappen gemist kan je met de rechtermuisknop op de server klikken en in het snelmenu op **Authorize**.

🛠 Klik met de rechtermuisknop op IPv4 en kies **New Scope**.

De scope bepaalt welke IP-adressen de DHCP server mag uitdelen. De New Scope Wizard leidt je door de verschillende instellingen.

- **Scope name**: geef een beschrijvende naam aan de scope en klik op Next.
- **IP Address Range**: Vul het eerste en laatste adres in dat de DHCP server mag uitdelen, evenals het aantal netwerkbits in de adressen en het subnetmasker. Klik op Next.

**Exclusions and Delay:** Adressen die binnen de opgegeven scope vallen en die al in gebruik zijn, b.v. omdat ze toegekend zijn aan een apparaat dat een vast IP-adres moet krijgen (een server, een printer ..), kunnen hier opgegeven worden. De DHCP server zal die adressen niet nog eens uitdelen.

Door de range van IP adressen in de scope en de range van vast gebruikte IP adressen gescheiden te houden, kan je ervoor zorgen dat Exclusions niet nodig zijn. Vind je het overzichtelijker om slechts met één range te werken dan kan je via de Exclusions dubbel gebruik van IP adressen voorkomen.

- **Add Exclusions and Delay**: Voeg indien van toepassing voor je huidige instellingen de nodige Exclusions toe.

Een client krijgt een IP adres slechts voor een beperkte tijd ter beschikking. De lease duration bepaalt hoelang.

Een lange lease duur heeft als resultaat dat toestellen lange tijd over hetzelfde IP adres zullen beschikken. Daarvoor wordt nogal eens gekozen in een stabiele omgeving waar weinig wisselende apparaten gebruikt worden. Een netwerk waarin de toestellen die deelnemen voortdurend wisselen (laptops, tablets, mobiele telefoons, ...) zal dan weer voordeel halen uit een korte lease tijd, omdat er sneller IP-adressen vrijkomen voor andere apparaten.

- **Lease Duration**: behoud de voorgestelde lease tijd.

Een DHCP server kan niet alleen IP adressen en subnetmaskers uitdelen aan zijn clients, maar kan meteen ook andere IP-instellingen meegeven, zoals het adres van de default gateway, het adres van de te contacteren DNS server, ... . Deze extra informatie wordt verspreid via de DHCP options.

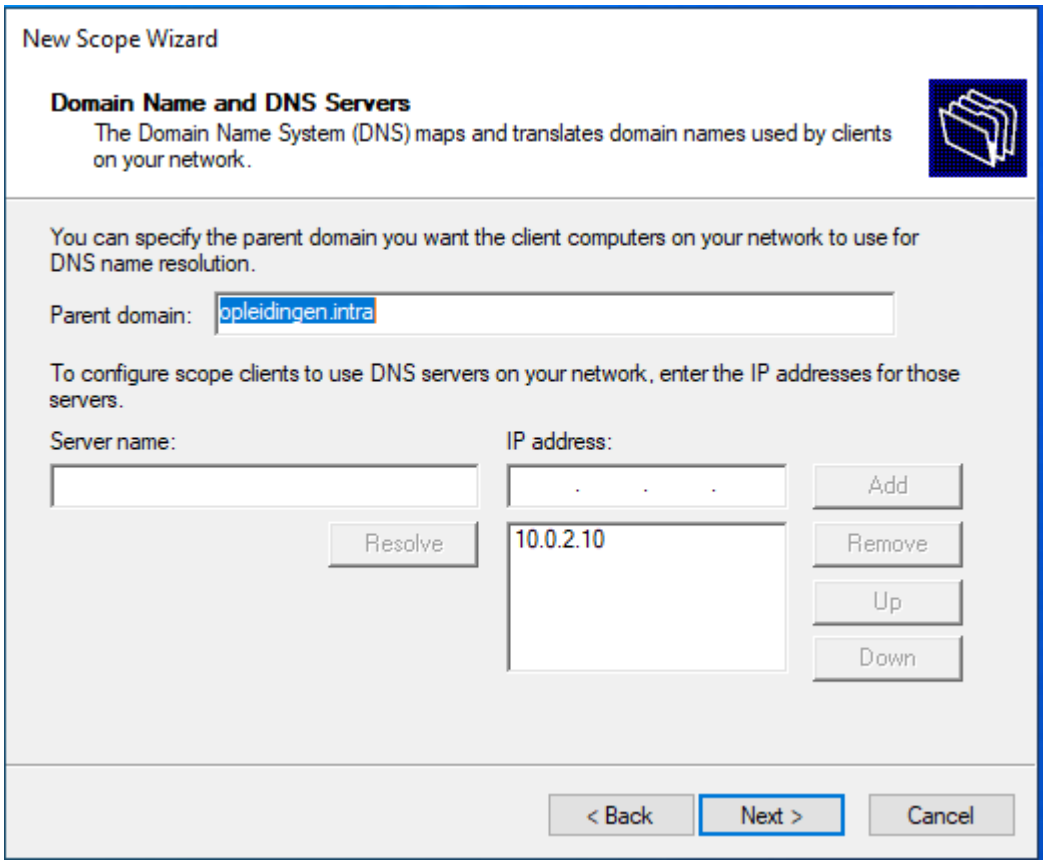
De opties kunnen ingesteld worden voor een bepaalde scope of op het niveau van de server. In dat geval tellen ze voor alle scopes.

- Selecteer **Yes, I want to configure these options now** en geef in de volgende dialoogvensters het adres van de router (**default gateway)** en het adres van de **DNS server(s)** mee.

**Let op:**

**Ook hier zijn de in de afbeeldingen getoonde instellingen louter als voorbeeld bedoeld. Om de IP-adressen te weten te komen die in jouw opstelling van toepassing zijn, kan je even stilstaan bij de informatie die je zou invullen bij**

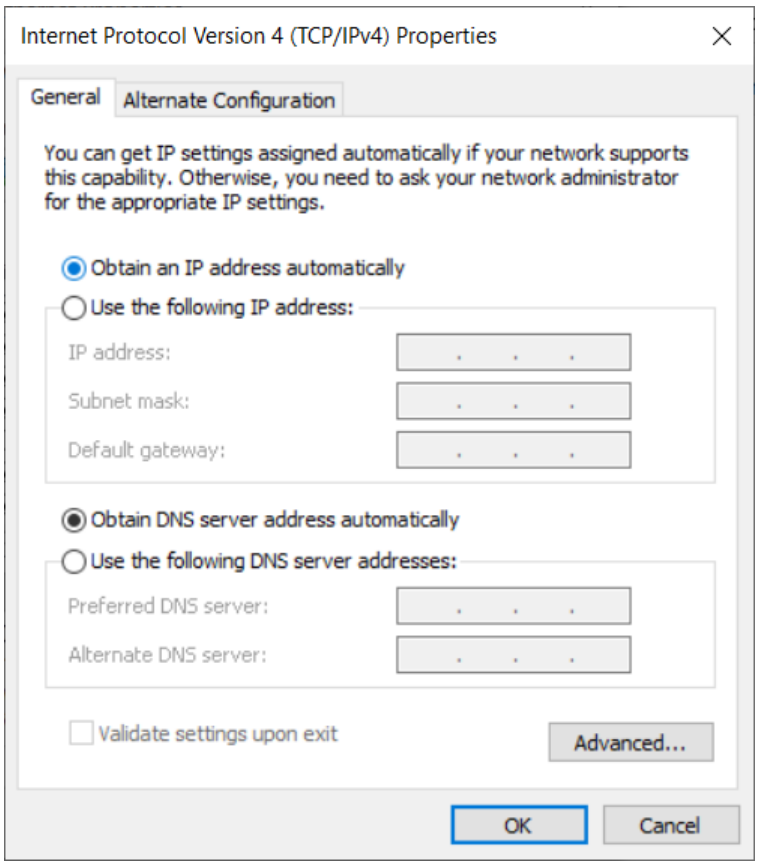
**een manuele configuratie. Bij IP-adres van DNS Server staat het adres van je domeincontroller.**




De volgende stap vraagt het adres van een WINS server op te geven. Een Wins server dateert nog van de tijd dat Windows systemen uitsluitend het NetBIOS protocol (niet TCP/IP) gebruikten om te communiceren binnen een LAN. WINS is verantwoordelijk voor de naamresolutie van NetBIOS namen.

- 🛠 Laat de instellingen ongemoeid.
- 🛠 Activeer in de laatste stap van de wizard de nieuw aangemaakt scope.

Configureer nu de client zo dat hij zowel een IP adres als een adres van een DNS server automatisch krijgt.




- Vraag aan de commandprompt je TCP/IP instelling op en check of ze inderdaad via de DHCP server geconfigureerd zijn. Je vraagt deze gegevens op via het commando **ipconfig /all** . De lijn die begint met “DHCP Server” geeft het IP adres van de server van wie je het IP adres gekregen hebt.

Het clienttoestel blijft hier als een lid van het domein functioneren. Je kan natuurlijk bij de installatie ook al onmiddellijk met dynamische IP-adressen werken.

# 5 APPENDIX: NAAMRESOLUTIE - DNS

IP Adressen zijn voor een computer optimaal om mee te werken. Zij vragen weinig processortijd bij verwerking, nemen weinig geheugenruimte in beslag en zijn snel transporteerbaar over een netwerk.

Voor de gebruiker is werken met IP adressen, zelfs in decimale notatie, echter niet echt voor de hand liggend.

Het adres http://www.vdab.be om naar de VDAB site te surfen is gemakkelijker te onthouden dan http://193.53.238.129.

Vanuit de applicatielaag wordt een computer dan ook meestal met een naam aangesproken.

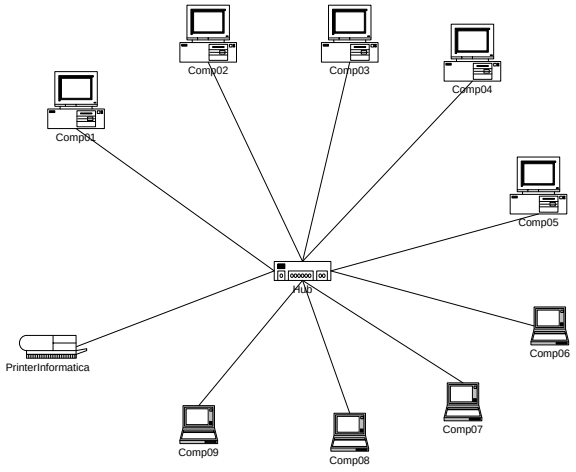
Ergens bij het doorlopen van de protocolstack moet er dan een omzetting gebeuren van een naam in een IP adres. Dergelijke omzetting wordt een naamresolutie genoemd.

## 5.1 Naamruimtes

Een naamruimte bepaalt de regels die gelden bij het geven van de namen: hoelang mogen of moeten de namen zijn, hoeveel verschillende namen zijn er maximaal mogelijk, welke karakters mogen gebruikt worden, ...

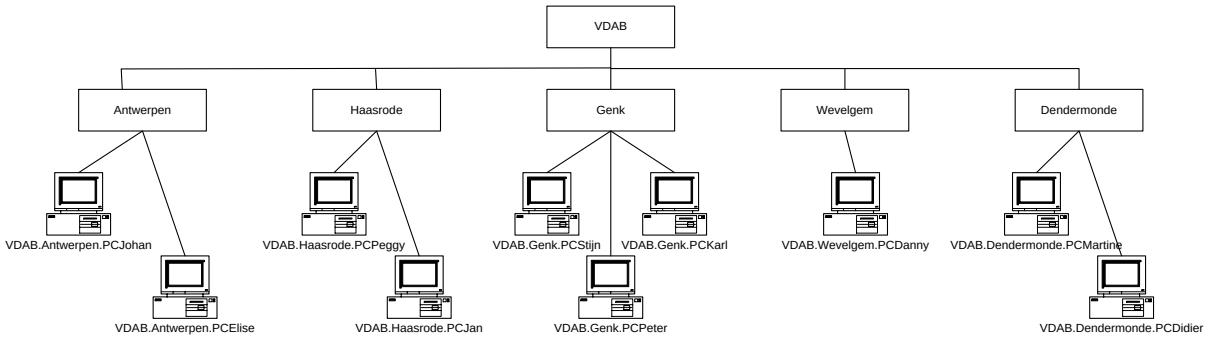
### 5.1.1 Vlakke naamruimtes

In een vlakke naamruimte worden namen gegeven zonder rekening te houden met een onderliggende structuur. Dergelijke naamruimtes zijn alleen geschikt voor kleine netwerken.




### 5.1.2 Hiërarchisch gestructureerde naamruimtes

In een hiërarchisch gestructureerde naamruimte bestaat een naam uit verschillende delen die volgens een bepaalde structuur achter elkaar worden gezet om tot de volledige naam te komen. Aan de hand van de samenstelling van de naam kan opgemaakt worden waar het toestel ergens in het internet thuishoort.




Een van de meest verspreide hiërarchische naamruimtes is de hiërarchische naamruimte waarmee TCP/IP werkt: DNS.

## 5.2 Naamregistratie

Naamregistratie legt de relatie tussen namen en adressen vast.

Omdat een computernaam ook gebruikt wordt om een toestel te identificeren, maar dan vanuit een applicatie, moet elk toestel op een internet ook een unieke naam krijgen.

Het registreren van namen hangt nauw samen met de structuur van de naamruimte. Voor een vlakke naamruimte moet de associatie tussen toestellen en namen centraal gebeuren, voor een hiërarchisch gestructureerde ruimte kan de verantwoordelijkheid verdeeld worden.

## 5.3 Naamresolutie met een Hostsbestand

Ten tijde van het ARPA net was het aantal aangesloten hosts nog erg klein. Om namen om te zetten in IP adressen werd een beroep gedaan op een ASCII-tekstbestand met de naam hosts.txt. Administrators haalden op regelmatige tijdstippen een nieuwe versie van het hosts bestand op en stelden die ter beschikking op de toestellen van hun netwerk.

Bij de installatie van Windows als besturingssysteem wordt nog altijd een standaard hosts bestand aangemaakt op de locatie c:\%systemroot%\system32\drivers\etc.

Het ziet er als volgt uit:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1       localhost
```

```
#      ::1             localhost
```

Op elke regel van het tekstbestand staat een IP adres gevolgd door een witruimte en dan de bijbehorende naam.

Een # duidt het begin van commentaar aan. Dat loopt tot het einde van de regel.

Onder Linux vind je een gelijkaardig bestand terug als /etc/hosts.

Met de uitbreiding van het Internet voldeed het hosts bestand niet meer. Het bestand werd groter en groter en was nooit echt up to date omdat er voortdurend nieuwe hostst bij kwamen. Bovendien moest elke naam uniek zijn. Het NIC had echter alleen zeggenschap over IP adressen en niet over namen van computers. Er werd gezocht naar een andere oplossing. Die werd gevonden in DNS, het domain name system.

## 5.4 Naamresolutie met DNS

### 5.4.1 De structuur achter DNS

Met de groei van het Internet werd op zoek gegaan naar een nieuw systeem waarin deze problemen opgelost werden. De oplossing werd in 1984 voorgesteld door Paul Mockapetris in de vorm van het Domain name system (DNS).

DNS bestaat uit een gedistribueerde database, dwz een database waarvan de inhoud verspreid zit over verschillende servers, naamservers genoemd.

Elke server is verantwoordelijk voor de informatie over bepaalde segmenten van het netwerk.

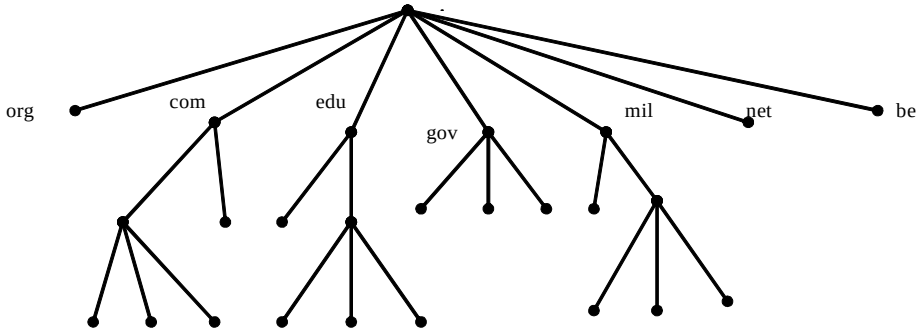
Clients of resolvers sturen via het netwerk queries naar de naamservers om bepaalde omzettingen te doen. Zo wordt de informatie beschikbaar op het volledige netwerk.

De hiërarchische opbouw lost het probleem van de naamoverlappingen op. Het distribueren van de database maakt het mogelijk lokale wijzigingen ook lokaal door te voeren.

Het Domain Name System werkt met een hiërarchische naamruimte waarin de verschillende delen van een naam van elkaar gescheiden worden door een punt en waarbij het meest specifieke deel van de naam vooraan te vinden is en het meer algemene deel achteraan.

#### 5.4.1.1 De theoretische structuur

De structuur van de gedistribueerde database is te vergelijken met de structuur van het bestandssysteem onder Windows of Linux (m.a.w een boomstructuur).




De structuur van het domain name sytem start bij de root, aangeduid met een punt (.).

Daaronder worden andere nodes gemaakt. Die nodes kunnen verantwoordelijk zijn voor bepaalde omzettingen en op hun beurt het beginpunt voor een nieuwe onderliggende structuur. Elke nieuwe structuur komt fysiek overeen met een partitie van de database en logisch met een domein in het domain name system.

Elk domein krijgt een unieke naam, opgebouwd op basis van de locatie in de database en te vergelijken met de absolute padnaam van een directory. Een absolute padnaam van een directory wordt echter opgebouwd van de root naar de directory (b.v. c:\Data\brieven of /usr/local/bin), de naam van een domein begint bij de naam van de node en wordt opgebouwd naar de root (cs.berkeley.edu.). Het deel tot aan het eerste punt, komt dus overeen met de naam van de pc, het vervolg correspondeert met de verschillende nodes tot aan de root. De domeinnamen worden als indexen gebruikt bij het doorzoeken van de database.

Bij het aanmaken van een structuur gelden een aantal spelregels die in de praktijk zelden of nooit een beperking zullen blijken:

- De boomstructuur mag maximaal 127 niveaus diep zijn.
- De naam van een node zonder punten mag maximaal 63 karakters lang zijn.
- Siblings, nodes die onder eenzelfde parent aangemaakt worden, moeten verschillende namen hebben. Dit garandeert meteen het uniek zijn van elke naam.

#### 5.4.1.2 De structuur van het Internet

Topdomeinen zijn domeinen die rechtstreeks onder de root aangemaakt zijn. Oorspronkelijk werd de Internet naamruimte opgedeeld in zeven topdomeinen geïnspireerd op de Amerikaanse maatschappij (ARPANet de voorloper van het Internet ontstond immers in Amerika). De creatie van deze topdomeinen valt onder de verantwoordelijkheid van het ICANN.

| | |
|---|---|
| Com | commerciële organisaties zoals Microsoft, HP, IBM, ... |
| Edu | organisaties die met vorming te maken hebben zoals universiteiten |
| Gov | gouvernementele organisaties zoals de NASA, de National Science Foundation, ... |

| | |
|---|---|
| Mil | militaire organisaties, het Amerikaanse leger, de Navy, ... |
| Net | oorspronkelijk organisaties die te maken hebben met netwerkvoorzieningen, sinds 1996 echter juist zoals com opengesteld voor alle commerciële organisaties |
| Org | oorspronkelijk voor niet commerciële organisaties, maar sinds 1996 ook toegankelijk voor allerlei organisaties |
| Int | internationale organisaties zoals de NATO |

Later (2001) werden hieraan toegevoegd aero, coop, museum, name, biz, info en pro om in te spelen op de snelle ontwikkeling van het Internet.

Andere landen waren natuurlijk ook vragende partij voor domeinnamen. Hierbij werd afgeweken van de indeling volgens type organisatie, maar werd gewerkt met de officiële afkorting van elk land die bepaald is in de ISO 3166 norm en die voor elk land uit twee letters bestaat (be=België, nl=Nederland enz.)

#### 5.4.1.3 Verdeling van de verantwoordelijkheden

Deze structuur maakt een verdeling van de verantwoordelijkheden mogelijk. Om een topdomein zoals edu te creëren is één keer de toelating nodig van de beheerders van het rootdomein, het ICANN. Om dan verder onder .edu een domein te creëren heb je de toelating nodig van de beheerders van het .edu domein, het ICANN komt hier niet meer bij kijken.

Zo ook in België. Het beheer van het .be domein was oorspronkelijk in handen van Professor Verbaeten verbonden aan de universiteit van Leuven. Naar aanleiding van de spectaculaire groei van het Internet werd die verantwoordelijkheid op 1 januari 2000 overgedragen aan een speciaal hiervoor opgerichte vereniging zonder winstoogmerk, DNS.be.

In de praktijk contacteer je echter je provider als je een domein onder be wilt creëren en beheren. Die zal zich op zijn beurt houden aan de afspraken die hij gemaakt heeft met DNS.be voor de registratie. Sinds eind 2000 mogen domeinnamen vrij gekozen worden, zolang ze maar uniek zijn. Onder je eigen node mag je een structuur uitbouwen zoals je zelf wilt, zonder dat je verder nog verantwoording naar buitenaf moet afleggen.

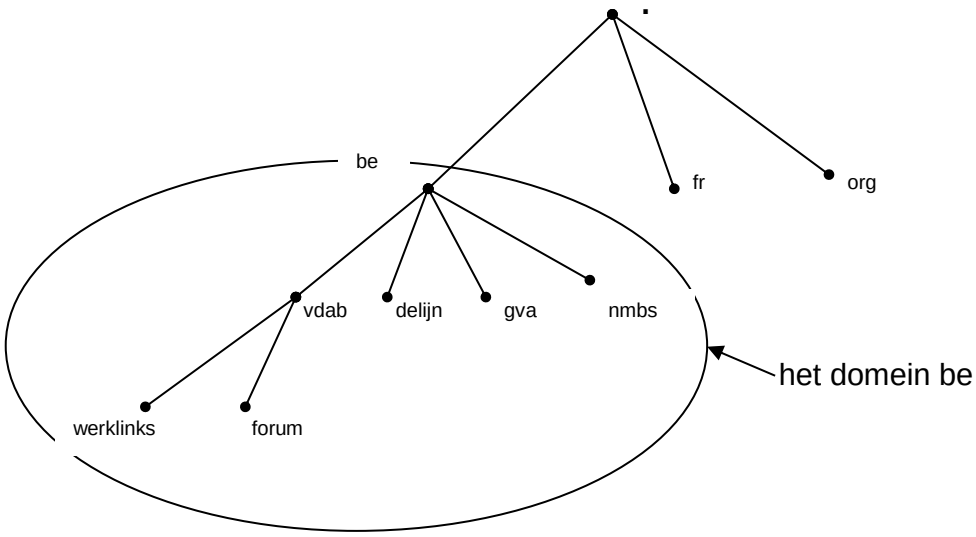
Je mag vanuit België uiteraard ook een nieuw domein aanvragen onder één van de topdomeinen in de Amerikaanse structuur.

### 5.4.2 Zones en domeinen

Tot nog toe werd alleen over domeinen gesproken. In de praktijk is een DNS server echter niet verantwoordelijk voor een domein, maar voor een aantal zones.

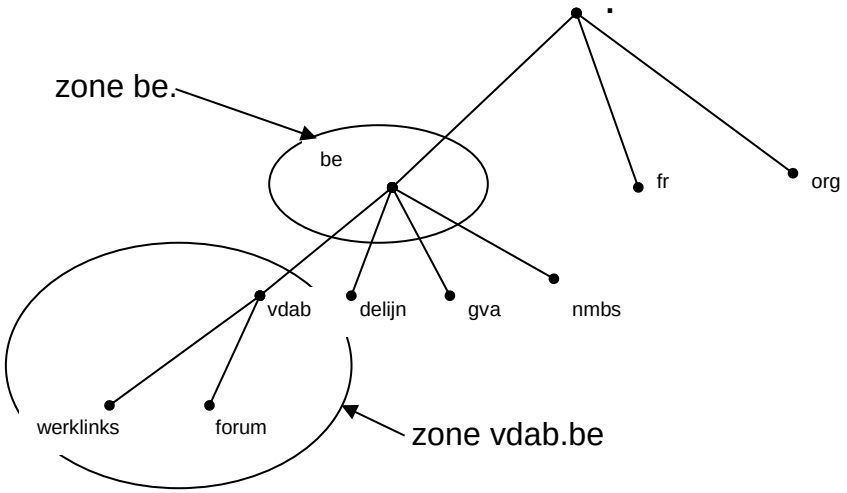
#### 5.4.2.1 Wat is een domein?

Een domein is de verzameling van alle hosts die onder een bepaalde node hangen.




5.4.2.2 Wat is een zone?

De naamserver van node be is niet noodzakelijk verantwoordelijk voor alle omzettingen in het domein be. Zo kunnen de naamomzettingen voor vdab.be gedelegeerd worden naar een naamserver die hoort bij de node vdab. Die kan op zijn beurt de omzetting voor werklinks.vdab.be delegeren naar nog een andere naamserver of zelf verantwoordelijk blijven voor die naamomzetting. De tekening hieronder illustreert hoe een naamserver de omzettingen voor vdab.be delegeert naar een andere naamserver bij de node vdab. Die naamserver is wel mee verantwoordelijk voor de omzettingen voor werklinks.vdab.be en forum.vdab.be.




Naamservers stockeren dus zones i.p.v. domeinen. Als een naamserver volledige domeinen zou stockeren zou dat te veel zijn.

### 5.4.3 Records

Een zone databestand is opgebouwd uit een aantal records. Naargelang de informatie die in een record opgeslagen is onderscheiden we o.a. volgende types records:

| | |
|---|---|
| A | Beeldt een host naam af op een IP adres |

| | |
|---|---|
| NS | Identificeert naamservers voor de zone |
| MX | Identificeert een mail server voor bepaalde machines of zones |
| SOA | Start of Authority, beschrijft de karakteristieken van een zone en wie gecontacteerd moet worden in geval van problemen. |
| CNAME | Laat toe een tweede naam te koppelen aan eenzelfde IP adres, m.a.w. een alias te creëren. |
| PTR | Pointer, beeldt een IP adres af op een naam. |

Administrators kunnen manueel records toevoegen aan een zone, maar dit is alleen zinvol als er een duurzame relatie bestaat tussen een hostnaam en een IP adres. Als een DHCP server de IP adressen toekent op een netwerk, moeten dynamische updates van de DNS records mogelijk zijn. De DHCP server kent in dat geval een IP adres toe aan een host en die registreert op zijn beurt zijn IP adres en naam bij de DNS server.

### 5.4.4 Hoe gebeurt een DNS naamomzetting?

#### 5.4.4.1 De rol van resolvers

Resolvers zijn clients die een naamserver contacteren om een naamomzetting uit te voeren. Programma's die een naamomzetting nodig hebben contacteren op hun beurt eerst een resolver. De resolver ontfermt zich dan over de volgende taken:

- Een query richten naar de naamserver.
- Een antwoord interpreteren (het antwoord kan bestaan uit een record of uit een foutmelding).
- Het bekomen antwoord doorspelen naar de aanvrager.

In dit scenario ligt het grootste deel van de verantwoordelijkheid voor de omzetting dus bij de naamserver. Dit type resolver wordt ook wel een stubresolver genoemd. In BIND (unixomgeving) is dit het type resolver dat het meest voorkomt.

#### 5.4.4.2 De rol van naamservers

De belangrijkste rol van een naamserver is dat hij de gevraagde omzettingen kan terugvinden in de naamruimte. Dit betekent dat hij niet alleen een antwoord moet kunnen vinden aan de hand van informatie waarvoor hij zelf verantwoordelijk is, maar ook aan de hand van informatie waarvoor andere naamservers verantwoordelijk zijn. Door de structuur van de naamruimte volstaat het dat de naamserver de naam en het IP adres van een root naamserver kan vinden. Een root naamserver kent de namen en IP adressen van de naamservers die verantwoordelijk zijn voor de top domeinen. De naamservers van de topdomeinen kunnen op hun beurt de namen en adressen bezorgen van de naamservers die rechtstreeks onder hun naamruimte vallen. En zo kan de boomstructuur telkens verder naar beneden doorzocht worden totdat de gewenste omzetting gevonden is.

#### 5.4.4.3 Naamservers voor de root zone

Je eigen DNS server moet dus niet alleen over de lokale informatie beschikken, maar moet ook de rootservers weten te vinden. Deze lijst is reeds ingebouwd in de meeste installaties van een DNS Server.

#### 5.4.4.4 Recursieve en iteratieve queries

Als er een omzetting moet gebeuren zal een resolver een recursieve query tot een door hem gekende naamserver richten. Een recursieve query is een query waarop als antwoord ofwel een omzetting ofwel een foutmelding verwacht wordt. Een referentie naar een andere naamserver is geen geldig antwoord op een recursieve query.

Er zijn nu twee mogelijkheden.

Ofwel kan de naamserver zelf rechtstreeks het antwoord leveren (b.v. omdat hij het in zijn cache vindt). In dat geval is daarmee de kous af. Het antwoord wordt bezorgd aan de client.

Ofwel kent de naamserver het antwoord niet. In dat geval gaat hij na of hij toevallig adressen kent van naamservers die hem al dichter bij het antwoord kunnen brengen. Om b.v. een naam als ***werklinks.vdab.be*** om te zetten zal de eerste naamserver nagaan of hij andere naamservers kent die verantwoordelijk zijn voor *werklinks.vdab.be*. Zo ja stuurt hij de query naar één van die naamservers en ontvangt de omzetting. Zo neen, gaat de eerste naamserver na of hij naamservers kent verantwoordelijk voor de omzetting van *vdab.be* en daarna voor *be*.

Als dit allemaal niet lukt moet de eerst gecontacteerde naamserver terecht bij een rootserver die hem in elk geval een referentie naar de naamservers verantwoordelijk voor **.be** zal kunnen bezorgen. De eerst gecontacteerde naamserver richt zich dan tot een naamserver verantwoordelijk voor be die hem op zijn beurt een referentie kan bezorgen naar een naamserver verantwoordelijk voor **vdab.be** enz.

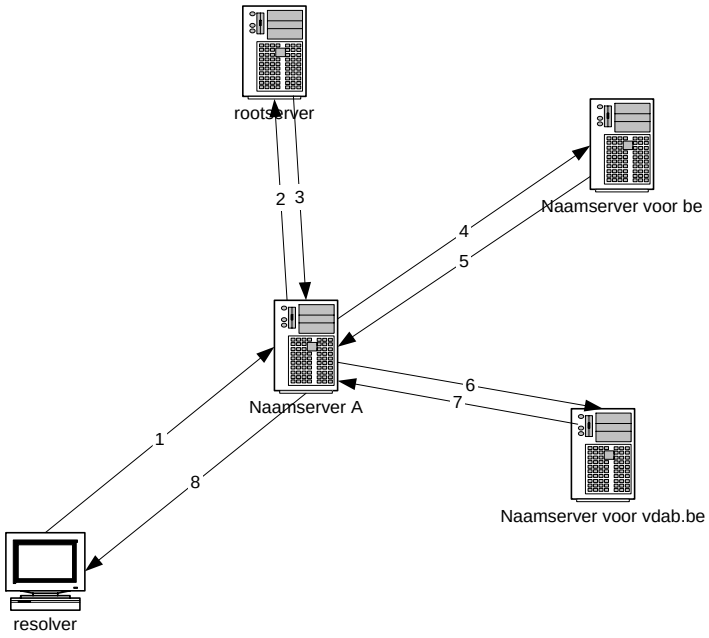
Een aantal opmerkingen bij deze procedure:

Uit dit verhaal blijkt dat de naamserver die eerst gecontacteerd werd door de resolver het merendeel van het werk op zich neemt. Die naamserver stuurt immers geen recursieve, maar iteratieve queries naar de andere naamservers. Een iteratieve query verwacht als antwoord ofwel een omzetting ofwel een referentie naar een andere naamserver die beter in staat is verder te helpen.

Een ander op te merken feit is dat door het opzoeken te starten bij een naamserver die verantwoordelijk is voor een naam zo dicht mogelijk bij de volledige naam het omzettingsproces zo kort mogelijk gehouden wordt.

Ten slotte zal de oorspronkelijk gecontacteerde naamserver telkens dezelfde query sturen als de resolver in eerste instantie naar hem heeft gestuurd. Dit om te vermijden dat er pogingen ondernomen worden om naar naamservers te zoeken die niet bestaan.

### 5.4.4.5 Schematische voorstelling




1. De resolver vraagt in een recursieve query aan A een omzetting van werklinks.vdab.be

2. A heeft zelf geen antwoord (zoekt daarbij in zijn cache naar werklinks.vdab.be, vdab.be en be en vindt voor geen van deze namen een omzetting) en stuurt een iteratieve query naar een rootserver met een vraag tot omzetting van werklinks.vdab.be.

3. De rootserver bezorgt referenties naar naamservers die zich ontfermen over de zone be.

4. A richt een iteratieve query tot een naamserver voor de zone be met een vraag tot omzetting van werklinks.vdab.be

5. A krijgt referenties naar naamservers verantwoordelijk voor de zone vdab.be.

6. A richt een iteratieve query tot een naamserver die verantwoordelijk is voor de zone vdab.be.

7. Deze naamserver bezorgt een omzetting van werklinks.vdab.be.

8. A stuurt het antwoord door naar de resolver.

### 5.4.4.6 Caching

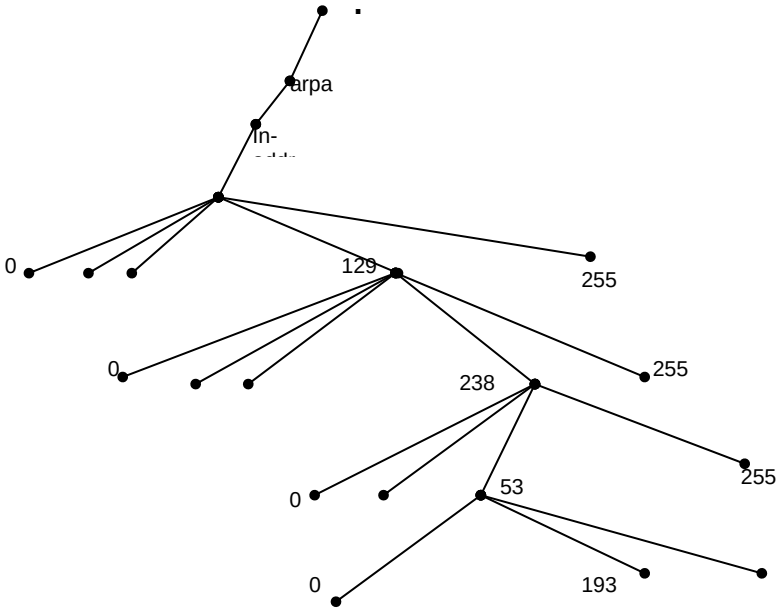
Deze procedure legt een grote werkdruk op de eerst gecontacteerde naamserver die een recursieve query ontvangt. Die werkdruk wordt erg verminderd door een systeem van caching. Tijdens het sturen van iteratieve queries komt de naamserver heel wat omzettingen te weten en adressen van naamservers die verantwoordelijk zijn voor bepaalde zones. Die informatie wordt tijdelijk opgeslagen in de cache van de naamserver, zodat hij op die informatie een beroep kan doen bij een volgende omzetting. Dit kan een belangrijke versnelling voor volgende omzettingen betekenen. Er worden niet alleen gevonden omzettingen in de cache opgeslagen, maar ook omzettingen die aanleiding gaven tot een foutmelding.

De inhoud van de cache moet natuurlijk wel op geregelde tijdstippen bijgewerkt worden, zoniet zouden wijzigingen op het netwerk nooit doordringen tot de naamservers. Hoe lang een omzetting of foutmelding geregistreerd blijft in de cache wordt bepaald door de time to live (ttl).

### 5.4.5 IP adressen omzetten in namen

Tot nog toe werd alleen stil gestaan bij het omzetten van namen in IP adressen. Het omgekeerde, IP adressen omzetten in namen kan ook nuttig zijn om uitvoer, zoals registraties in logbestanden, beter leesbaar te maken. De structuur van DNS maakt het opzoeken van namen vrij eenvoudig omdat de namen als indexen gebruikt worden in de database. Het opzoeken van IP adressen in diezelfde structuur betekent echter de structuur volledig doorlopen. Daarom kan aan een naamruimte ook een zone gekoppeld worden waar de nodes aan de hand van IP adressen geïdentificeerd worden. Dit wordt de reverse lookup zone genoemd.

De structuur van deze ruimte ziet er dan als volgt uit:




Hier wordt b.v. het pad naar IP adres 193.53.238.129 (www.vdab.be) gevolgd. Merk op dat de IP adressen van achter naar voor opgezocht worden. Dit is in overeenstemming met de manier waarop naar namen gezocht wordt, namelijk van meer specifiek naar meer algemeen. Daar waar het algemene gedeelte van een naam echter achteraan staat, komt het netwerkadres in een IP adres overeen met het voorste deel. Op die manier blijft het ook voor IP adressen mogelijk de verantwoordelijkheden voor de lokale omzettingen bij de lokale administrator te leggen.

# 6 COLOFON

| | |
|---|---|
| **Sectorverantwoordelijke:** | |
| **Cursusverantwoordelijke:** | Bjorn Smeets |
| **Didactiek:** | |
| **Lay-out:** | |
| **Medewerkers:** | Vakgroep systeembeheer |
| **Versie:** | December 2024 |
| **Nummer dotatielijst:** | |